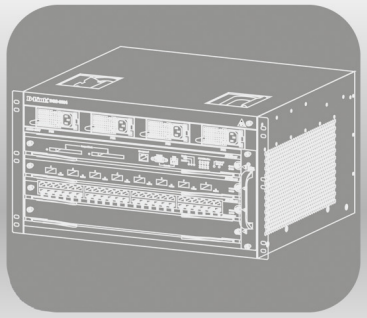


CLI Reference Guide

Product Model: DGS-6600 Series
Modular Layer 3 Chassis Ethernet Managed Switch
Software Release: 2.00

DGS-6604 CLI Reference Guide

Software Release 2.00.022

Date: November 3, 2011

Copyright Statement

Preface

Version Description

This manual's command descriptions are based on the software release 2.00.022. The commands listed here are the subset of commands that are supported by the DGS-6600 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-6604 by using the D-LINK Command Line Reference (CLI). The CLI is the primary management interface to the D-LINK DGS-6604 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 Organiztion

Preface	Describes how to use the CLI reference manual.
Feature Table of Contents	A clickable commnad list of the DGS-6604 commands grouped by their features and linked to the command descriptions..
Command Listings	A complete list of available commands arranged in alphabetical order.
Acronyms	A glossary of acronyms used througout the reference manual.

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-6600 Series Quick Installation Guide
- DGS-6600 Series Hardware Installation Guide

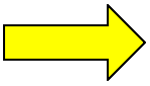
Conventions

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 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 consise 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 v 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 vi 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 four privilege levels:

- **Basic User**- Privilege Level 1. This user account level has the lowest priority of the user accounts and is allowed to configure the terminal control settings. The purpose of this type of user account level is for basic system checking. This user account can only show limited information that is not related to security. The most important limitation of this account is that there is no way of changing the access right level.
- **Advanced User**- Privilege Level 2. This user account level is very similar to a basic user except that an advanced user can enter privileged EXEC mode.
- **Power User**- 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:

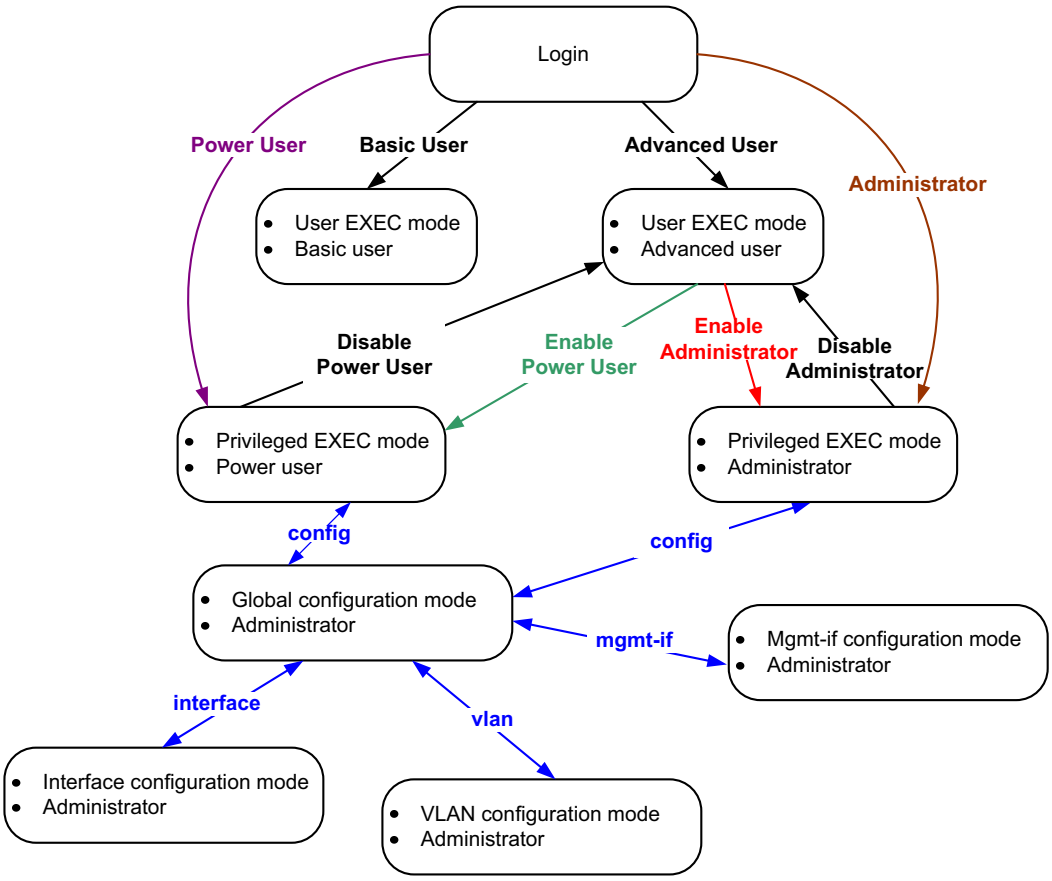
- **User EXEC mode**
- **Privileged EXEC mode**
- **Global Configuration mode**

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 and advanced user level will log into the Switch in user EXEC mode. Users with power user and administrator level accounts will log into the Switch in privileged EXEC mode. Therefore, user EXEC mode can operate at either basic user level or advanced user level, and privileged EXEC mode can operate at either power user level 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 power user 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.

In user EXEC mode at advanced user level, the user is allowed to enter privileged EXEC mode by entering the enable password. In privileged EXEC mode, the user is allowed to exit to the user EXEC mode at advanced user level by entering the **disable** command. The **enable password** and **disable** commands are functions that can be used to switch between user EXEC mode and privileged EXEC mode.

The following state diagram describes the main command modes and how to enter each one:



Note: Not all configuration modes are listed in the above figure. For example, in global configuration mode, enter **"router ospf"** to enter OSPF router configuration mode

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	For checking basic system settings, allowing users to change the local terminal session settings, and verifying basic network connectivity. Checking security related settings is not allowed at this command mode and privilege level.
User EXEC mode at Advanced User level	This level has almost the same access rights as user EXEC mode at basic user level, except that a user in this mode and at this level can enter privileged EXEC mode by entering the **enable** command.
Privileged EXEC mode at Power User 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, 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.
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 Power User level	For applying interface related settings.

Command Mode & Privilege Level	Purpose
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, allowing users to change the local terminal session settings and carry out basic network connectivity verification. One limitation of this command mode is that it cannot be used to display information related to security. 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.

User EXEC Mode at Advanced User Level

User EXEC mode at advanced user level has the same purpose as user EXEC mode at basic user level, except that user EXEC mode at advanced user level is allowed to use the **enable** command to enter privileged EXEC mode.

This command mode can be entered by logging in as an advanced user or by using the **disable** command in privileged EXEC mode.

In the following example, the user is currently logged in as an advanced user in privileged EXEC mode and uses the **disable** command to return to user EXEC mode at advanced user level:

```
DGS-6604:15#disable
DGS-6604:2>
```

Privileged EXEC Mode at Power User 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.)

There are two methods that a user can use to enter privileged EXEC mode at power user level. The first method is to login to the Switch with a user account that has a privilege level of 12. The other method is to use the **enable privilege *LEVEL*** command in user EXEC mode.

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-6604 Chassis-based High-Speed Switch
                             Command Line Interface

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

DGS-6604:12#
```

In the following example, the user enters the **enable privilege *LEVEL*** command in user EXEC mode to enter privileged EXEC mode at Power User level:

```
DGS-6604:2>enable privilege 12
DGS-6604:12#
```

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.

There are two methods that a user can use to enter privileged EXEC mode at administrator level. The first method is to login to the Switch with a user account that has a privilege level of 15. The second method requires a user to login to the Switch in as a user with an advanced user or power user level and and use the **enable privilege *LEVEL*** command.

In this command mode, the user can return to user EXEC mode at an advanced user level by entering the **disable** command.

In the following example, the user is currently logged in as an administrator in privileged EXEC mode and uses the **disable** command to return to user EXEC mode at an advanced user level:

```
DGS-6604:15#disable
DGS-6604:2>
```

In the following example, the user enters the **enable privilege *LEVEL*** command in privileged EXEC mode at power user level to enter privileged EXEC mode at an administrator level:

```
DGS-6604:12#enable privilege 15
DGS-6604:15#
```

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-6604:15#configure terminal
DGS-6604:15(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-6604:15(config)#interface vlan*VLAN-ID*	Enters VLAN interface configuration mode.

Command Listing by Feature

802.1x

AAA

Access Control Lists

Access Management

OSPFv3

Password Recovery

PIM

QinQ (VLAN Tunnel)

aaa authentication

Use this command to enable the AAA authentication function (console, telnet, ssh or http) using the method or methods specified and to create a login list to specify the application or applications used for system access.

Note: Use **aaa group server** to first define authentication servers before aaa authentication can be configured.

aaa authentication [login | enable] [console | telnet | http | ssh] *METHOD1* **[** *METHOD2***...]**

no aaa authentication [login | enable] [console | telnet | http | ssh] *METHOD1* **[** *METHOD2...***]**

Syntax Description	
login	(Optional) Enable authentication for normal login mode. Enter the console, telnet, or http keyword. If neither login nor enable are specified, both login and enable are implied.
enable	(Optional) Enable authentication for normal enable mode. Enter the console, telnet, or http keyword. If neither login nor enable are specified, both login and enable are implied.
console	(Optional) Specifies that the type of application used for system access authentication is console.
telnet	(Optional) Specifies that the type of application used for system access authentication is telnet.
http	(Optional) Specifies that the type of application used for system access authentication is http.
ssh	(Optional) Specifies that the type of application used for system access authentication is SSH.
METHOD1 [METHOD2...]	Identifies the list of methods that the authentication algorithm tries in the given sequence. At least one method must be entered; up to two methods can be identified by keyword. The keywords for AAA authentication login and enable configuration methods are described as follows: • **local** Uses the local username database for authentication. • **group** *GROUP-NAME* Uses a subset of authentication servers for authentication as defined by the **aaa group server** command.

Default No aaa authentication, **local** user authentication is specified for console, telnet, http, etc. application.

Command Mode Global configuration at privilege level 15

Usage Guideline Use aaa authentication to enable authentication and create a login list to specify the application or applications used for system access.

If neither login or enable are specified, both are implied. If no application is specified, all applications (console, telnet,ssh, or http) are assumed valid for sytem access.

Multiple methods for the login/enable authentication per application can be specified. The new setting will overwrite the old association.

Use **no aaa authentication** to disable authentication for system access or to disable the login list of applications used for system access.

To configure AAA authentication, first define a group of authentication servers (use **aaa group server** command). If a specified group server cannot be found, an error message is displayed. The group server defines the type of authentication to be performed and the sequence in which they will be performed.

A method list describes authentication methods used in the sequential order listed. The method defines a security protocol, if any is used, for user authentication. More than one method can be defined to provide a backup authentication procedure. If the first method cannot be used or there is no response, the next method listed is used and so on for up to 2 defined methods. The process continues until either the user is authenticated successfully, or all methods listed are exhausted.

Note that if, at any point, access is denied by an authentication method employed, the authentication process is stopped, no more methods are eligible and no other attempts to authenticate are made.

The **local** method for authentication uses locally configured login and enable passwords to authenticate login attempts. The login and enable passwords are local to each switch and are not mapped to the individual user names. The local method is used by default for authentication if no method is listed. If a differnet authentication method is listed for login or enable, the switch will not attempt local authentication.

In order to use AAA authentication, at least one local user account for login must first be created and the enable password set up.

Example

The following example sets a login method list for an authenticate login attempt from all of the applications (including console, telnet, ssh, http). The methods start from group2.

```
Switch(config)# aaa authentication login group group2 local
Switch(config)#
```

Verify the settings by entering the **show aaa** command.

aaa authorization

Use this command to enable the authorization function. Use the no form of the command to disable AAA authorization.

aaa authorization

no aaa authorization

Syntax None

Default Disabled

Command Mode Global configuration at privilege level 15

Usage Guideline When the AAA authorization function is enabled, the system will use configuration settings authorized by the RADIUS server in addition to the RADIUS server authentication function. Settings can include VLAN assignment, user priority assignment and bandwidth assignment.

If AAA authorization is disabled, the system only accepts the authentication function from the RADIUS server and ignore any additional configuration settings supplied by the RADIUS server.

Example This example shows how to enable the authorization:

```
Switch# configure terminal
Switch(config)# aaa authorization
```

Verify the settings by entering the **show system protocol-state** command.

aaa group server

Use the aaa group server command to enter AAA group server mode and identify AAA server groups used for AAA authentication. In AAA group server mode server hosts are grouped into distinct lists and distinct methods.

To remove a group server from the configuration list, use the no aaa group server form of this command.

aaa group server *GROUP-NAME*

no aaa group server *GROUP-NAME*

Syntax Description	
GROUP-NAME	Character string used to name the group of servers used for group server method AAA authentication. The group name can be up to 32 characters in length.

Default There is no aaa group server.

Command Mode Global configuration at privilege level 15

Usage Guideline The AAA group server method is defined for AAA authenticatication for user login or configuration. The **aaa authentication** command is used to define the group server method and specify the AAA server group.

Use **aaa group server** command to enter AAA group server mode. If the group name specified does not exist, the switch creates the new group. Once in AAA group server mode, use the **server** command to define and configure servers added to the group.

Example The following example shows the network access server configured to recognize two RADIUS host entries. The second host entry configured acts as fail-over backup to the first one. (The RADIUS host entries are tried in the order in which they are configured.)

```
Switch(config)#aaa group server group1
Switch(config-aaa-groug-server)# server radius 172.19.10.100 key 12345678
Switch(config-aaa-group-server)# server radius 172.19.10.200 key 12345678
Switch(config-aaa-group-server)# end
Switch#
```

Verify the settings by entering the **show aaa group server** command.

accept dhcp client-identifier

Use this command to turn on validation checking of the Client Identifier. Use the no form of the command to turn off validation checking of the Client Identifier.

accept dhcp client-identifier

no accept dhcp client-identifier

Syntax None

Default **client identifer**: not evaluated

Command Mode DHCP pool configuration

Usage Guideline To validate the DHCP Client Identifier value sent by the client. If a DHCP client sends a DHCP Client Identifier option, the DHCP server validates the value to ensure it matches the hardware type and client hardware address. If the values match, the DHCP server provides service to the client. If the values do not match, the DHCP server does not respond to the client's request.

If the command is used to set the validation to not check the DHCP Client Identifier value sent by the client, then the DHCP server only checks the matching of the client's hardware type and hardware address as a host ID.

Example The following example sets the DHCP pool1 to check the validation of the client identifier option as DHCP pool1 offers IP addresses.

```
switch > enable
switch# configure terminal
switch(config)# ip dhcp pool pool1
switch(config-dhcp)# accept dhcp client-identifier
switch(config-dhcp)#
```

accept dhcp relay-agent

To accept relay agent information use the accept dhcp relay-agent command, use the no form of the command to reject DHCP relay agent information.

accept dhcp relay-agent [circuit-id|remote-id]

no accept dhcp relay-agent [circuit-id|remote-id]

Syntax Description	
circiut-id	(Optional) Agent Circuit ID Sub-option.
remote-id	(Optional) Agent Remote ID Sub-option

Default DHCP relay-agent is not accepted.

Command Mode DHCP pool configuration

Usage Guideline If either of circuit-id and remote-id is not specified, it implys that both the circuit-id and remote-id options are applied with the command. If only the circuit-id or remote-id is specified, it implies that it only accepts DHCP packets containing either only a circuit-id or a remote-id.

Examples The following example sets DHCP pool1 to accept circuit id and remote id relay agent information.

```
switch > enable
switch# configure terminal
switch(config)# ip dhcp pool pool1
switch(config-dhcp)# accept dhcp relay-agent
switch(config-dhcp)#
```

The following example sets DHCP pool1 to not accept remote id relay agent information.

```
switch > enable
switch# configure terminal
switch(config)# ip dhcp pool pool1
switch(config-dhcp)# no accept dhcp relay-agent remote-id
switch(config-dhcp)#
```

acceptable-frame

Use the **acceptable-frame interface** command to set the acceptable frame type of a port for IEEE 802.1Q VLANs. The default acceptable frame type is admit-all.

acceptable-frame { tagged-only | untagged-only | admit-all }

Syntax Description	
tagged-only	Set acceptable frame type for tagged only of the interface.
untagged-only	Set acceptable frame type for untagged only of the interface.
admit-all	Set acceptable frame type for all packets of the interface.

Default **admit-all**

Command Mode interface configuration

Usage Guideline The valid interfaces for this command are physical ports.

The acceptable-frame interface command can be used to set the acceptable frame types for physical port interfaces. If an acceptable frame type is **tagged-only**, only tagged packets of incoming packets will be received by the interface and untagged packets will be dropped. If **untagged-only**, only untagged packets will be received and tagged packets will be dropped. If **admit-all**, all packets will be received.

Example This example shows how to set the acceptable frame type to tagged-only of eth3.1.

```
Switch(config)# interface eth3.1
Switch(config-if)# acceptable-frame tagged-only
```

Verify the settings by entering the **show vlan interface** command.

accept-lifetime

The accept-lifetime command is used to set a time period when an authentication key on a key chain is accepted as the valid key.

accept-lifetime *START-TIME* **{ infinite |** *END-TIME* **| duration** *SECONDS* **}**

Syntax Description	
START-TIME	The beginning time that the key specified, by the key command, is valid to be received. The syntax can be either of the following: HH:MM:SS MONTH DATE YEAR HH:MM:SS DATE MONTH YEAR HH-hours MM-minutes SS-seconds MONTH-first three letters of the month DATE-date (1-31) YEAR-year (four digits) The default start time and the earliest acceptable date is January 1, 1993.
infinite	Key is valid to be received from the start-time value on.
END-TIME	Key is valid to be received from the start-time value until the end-time value.The syntax is the same as that for the START-TIME. The end-time value must be after the start-time value. The default end time is an **infinite** time period.
duration *SECONDS*	Length of time (in seconds) that the key is valid to be received. The range is from 1 to 2147483647 (signed long).

Default Infinite

Command Mode Key-chain key configuration

Usage Guideline Only Routing Information Protocol (RIP) Version 2 uses key chains.

Specify a start time value and one of the following values: infinite, end-time, or duration seconds.

Example

The following example configures a key chain named chain1. Key 1 named "forkey1string" will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. Key 3 named "forkey3string" will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m.

```
Switch(config)# interface vlan1
Switch(config-if)# ip rip authentication key-chain chain1
Switch(config-if)# ip rip authentication mode text
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 172.19.0.0/8
Switch(config-router)# version 2
Switch(config-router)# exit
Switch(config)# key chain chain1
Switch(config-keychain)# key 1
Switch(config-keychain-key)# key-string forkey1string
Switch(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2009 duration 7200
Switch(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2009 duration 3600
Switch(config-keychain-key)# exit
Switch(config-keychain)# key 3
Switch(config-keychain-key)# key-string forkey3string
Switch(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2009 duration 7200
Switch(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2009 duration 3600
Switch(config-keychain-key)# exit
Switch(config-keychain)# exit
```

Verify the settings by entering the **show ip key-chain** command.

access vlan

Use the **access vlan** interface configuration command to specify the access VLAN for the interface. Use **default interface vlan** command to reset to default setting.

access vlan *VLAN-ID*

default access vlan

Syntax Description	
access vlan	Specifies the access VLAN for the interface.
VLAN-ID	

Default VLAN 1

Command Mode Interface configuration

Usage Guideline The command is valid for physical ports or port-channel interfaces. If the VLAN does not exist, the VLAN will be automatically created and a message pompt will appear. By default, the port has access VLAN 1.

The following applies to access VLANs:

- An interface can be specified with only one access VLAN. The succeeding command overwrites the previous command.
- When this command is applied, the port will change to Access mode. If the port has been configured for other modes, Access mode will overwrite the previous mode. The port's PVID is changed to the specified VLAN.

Examples This example shows how to set an interface eth3.1 to an untagged member of VLAN 1000.

```
Switch(config)# interface eth3.1
Switch(config-if)# access vlan 1000
```

Verify the settings by entering the **show vlan interface** command.

address-family ipv4

Use this command to enter *address family* configuration mode to configure a routing session using standard IP Version 4 address prefixes. Use the **no** form of this command to remove the IPv4 *address family* configuration from the running configuration.

address-family ipv4 [unicast]

no address-family ipv4 [unicast]

Syntax Description	
unicast	(Optional) Specifies IP Version 4 unicast address prefixes.

Default

Unicast prefix support is enabled by default when this command is entered without any optional keywords.

Command Mode

Router configuration

Usage Guideline

Routing information for address family IPv4 unicast is advertised by default for each BGP routing session configured with the **neighbor remote-as** command unless the **no bgp default ipv4-unicast** command is used before configuring the **neighbor remote-as** command.

For all settings configured for IPv4 unicast, the settings also appear in *BGP router* configuration mode. That is, for *address-family* associated settings, the settings defined in IPv4 unicast *address family* mode is equivalent to the settings defined in the *router* configuration mode.

To leave *address family* configuration mode and return to *router* configuration mode without removing the existing configuration, enter the **exit** command.

Example

This example shows how to enter address family configuration mode for the IP Version 4 address family:

```
Switch(config)# router bgp 65100
Switch(config-router)# address-family ipv4
Switch(config-router-af)# exit
Switch(config-router)#
```

aggregate-address

Use this command to configure BGP aggregate entries. Use the no form of the command to disable this function.

aggregate-address *NETWORK-NUMBER/SUBNET-LENGTH* **[summary-only] [as-set]**

no aggregate-address *NETWORK-NUMBER/SUBNET-LENGTH* **[summary-only] [as-set]**

Syntax Description	
NETWORK-NUMBER/ SUBNET-LENGTH	Specifies the number of network and the length of network that BGP will aggregate. The format of NETWORK-NUMBER/SUBNET-LENGTH 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 Disabled

Command Mode Router configuration

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.

The **as-set** parameter creates an aggregate entry advertising the path for this route, consisting of all elements contained in all paths being summarized. Use the **as-set** parameter to reduce the size of the path information by listing the 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 an incomplete path information.

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

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

area default-cost

The cost of the default summary route sent into a *not-so-stubby area* (NSSA) or a stub area is defined with the **area default-cost** command in *router* configuration mode. The **no area default-cost** command is used to remove an assigned default route cost.

area *AREA-ID* **default-cost** *COST*

no area *AREA-ID* **default-cost**

Syntax Description	
AREA-ID	Identifier for the NSSA or stub area. The identifier is specified as either a decimal value or as an IPv4 prefix. COST is not Optional.
COST	*COST* for the default summary route used for a stub or NSSA. The acceptable value is a 24-bit number (0~16777215).

Default *COST*: 1

Command Mode Router configuration

Usage Guideline Use this command only on an Area Border Router (ABR) attached to a stub area or NSSA.

The two stub area router configuration commands are **area stub** and **area default-cost** are configured as follows: for all routers and access servers attached to the stub area, the area should be configured as a stub area using the **area stub option**; the **area default-cost** command is used only on an ABR attached to the stub area. The **default-cost** provides the metric for the summary default route generated by the ABR into the stub area.

Example The following example assigns a default cost of 20 to stub network 10.0.0.0

```
Switch# configure terminal
Switch (config)# router ospf
Switch (config-router)# area 10.0.0.0 default-cost 20
```

Verify the settings by entering the **show ip ospf interface** command.

area default-cost (IPv6)

To set the summary-default cost of a stub area, use the **area default-cost** command. To disable this function, use the no form of this command.

area *AREA-ID* **default-cost** *COST*

no area *AREA-ID* **default-cost**

Syntax Description	
AREA-ID	Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IPv4 prefix.
COST	(Optional) Metric or cost for this summary route, which is used during the OSPF SPF calculation to determine the shortest paths to the destination. The value can be 0 to 16777215.

Default Disabled

Command Mode Router configuration

Usage Guideline This command is used only on an Area Border Router (ABR) attached to a stub area. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the stub option of the area command. Use the **area default-cost** command only on an ABR attached to the stub area. The **default-cost** option provides the metric for the summary default route generated by the ABR into the stub area.

Examples The following example assigns a default cost of 10 to stub area 1.

```
Switch > enable
Switch # configure terminal
Switch (config) # router ipv6 ospf
Switch (config-router) # area 1 stub
Switch (config-router) # area 1 default-cost 10
```

area nssa

Use this command to define an area as an NSSA (not-so-stubby) area. Use the **no nssa** command to remove the NSSA designation.

Note: For OSPFv3 this command is not supported.

area *AREA-ID* **nssa [no-redistribution] [default-information-originate [metric** *METRIC-VALUE***] [metric-type** *TYPE-VALUE* **]] [no-summary]**

no area *AREA-ID* **nssa [no-redistribution] [default-information-originate] [no-summary]**

Syntax Description	
AREA-ID	Specifies the identifier of the area distinguished as the NSSA. The identifier can be specified as either a decimal value or an IP address.
no-redistribution	(Optional) Type 7 external routes will not be re-distributed to the NSSA. When the user specifies to redistribute routes to the OSPF process, external routes will always be redistributed to the normal area. This function only takes effect when the router is an autonomus sytem boundry router (ASBR).
default-information-originate	(Optional) For ASBR, a Type 7 default route will be generated into the NSSA area when it exists in the redistributed routes. For ABR, when this option is specified, the type-7 default route will always be generated into the NSSA area.
metric *METRIC-VALUE*	(Optional) Specifies the metric for the default route. If not specified, the value will be 1. The range for *METRIC-VALUE* is 0-16777214.
metric-type *TYPE-VALUE*	(Optional) For OSPF, the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values: Type 1 external route or Type 2 external route. If a metric-type is not specified, the switch adopts a Type 2 external route.
no-summary	(Optional) This function only take effect when the router is an ABR. Summary routes are not advertised into the NSSA.

Default

- No NSSA area is configured.
- External routes will be redistributed to the NSSA area in type 7 unless **no-redistribute** is specified.
- Type 7 default route will only be advertised by default when **default-information-originate** is specified.
- If **no-summary** is specified, the summary route will not be advertised to the NSSA area.

Command Mode Router configuration

Usage Guideline There are no external routes in an OSPF stub area, so it is not possible to redistribute from another protocol into a stub area.

An NSSA allows external routes to be advertised to the area in type 7 link state advertisement (LSA). These routes are then leaked into other areas. Although, the external routes from other areas still do not enter the NSSA.

Use the **area nssa** command to simplify the administration of connecting a central site using OSPF to a remote site that is using a different routing protocol. Use this command to extend OSPF to cover the remote connection by defining the area between the central router and the remote router as an NSSA.

For ASBR NSSA re-distribution, external routes will only be redistributed to the NSSA when redistribution is configured for the associated OSPF process.

The external routes from other areas within the same AS will not be injected to the NSSA.

For an ASBR, a Type 7 default route will be generated into the NSSA when it exists in the redistributed routes.

For an ABR, when this option is specified, the type-7 default route will always be generated into the NSSA.

If there are multiple default routes generated into the NSSA, the following priority will be followed: Type 3 priority > Type 7 priority.

Example

This command show how to set the nssa area:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 1 nssa
```

Verify the settings by entering the **show ip ospf** command.

area range

Use this command to summarize and consolidate routes at an area boundary. Use the **no area range** command to disable this function.

area *AREA-ID* **range** *PREFIX/PREFIX-LENGTH* **[advertise | not-advertise] [cost** *COST***]**

no area *AREA-ID* **range [***PREFIX/PREFIX-LENGTH* **]**

Syntax Description	
AREA-ID	Specifies the identifier of the area for which routes are summarized. The identifier can be specified as either an IP address or a decimal value.
PREFIX/PREFIX-LENGTH	The prefix and length of prefix for the area range.
advertise	(Optional) Sets the status to advertise and generate a Type 3 summary link-state advertisement (LSA) for the specified address range.
not-advertise	(Optional) Sets the status to DoNotAdvertise for the specified address range. Type 3 summary LSA is suppressed, the component networks remain hidden.
COST	Cost for speicified summary route. The valid setting is 0 to 16777215.

Default Disabled

The default is advertise.

If cost is not specified, the cost of this route is found from the cost sets of component subnets and the maximum cost of those is chosen. (based on RFC2328).

Command Mode Router configuration

Usage Guideline Use this command with ABRs to summarize the intra-area routes. This command is used to specify the summarized route for area 0 or for a non-zero area.

Multiple area router configuration commands specifying the range option can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

For the same area, this command can also be specified multiple times.

Example This example shows how to set one summary route to be advertised by the ABR to other areas for all subnets on network 192.168.0.0:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 1 range 192.168.0.0/16
```

Verify the settings by entering the **show ip ospf** command.

area range (IPv6)

To consolidate and summarize routes at an area boundary, use the **area range** command. To disable this function, use the no form of this command.

area *AREA-ID* **range** *IPv6-PREFIX/PREFIX-LENGTH* **[advertise | not-advertise]**

no area *AREA-ID* **range** *IPv6-PREFIX / PREFIX-LENGTH*

Syntax Description	
AREA-ID	Identifier of the area for which routes are to be summarized. It can be specified as either a decimal value or as an IPv4 prefix.
IPv6-PREFIX	IPv6 prefix
PREFIX-LENGTH	IPv6 prefix length
advertise	(Optional) Advertise and generate a Type 3 Inter-Area Prefix link-state advertisement (LSA) for the specified address range.
not- advertise	(Optional) Sets the status to *DoNotAdvertis*e for the specified address range. The Type 3 Inter-Area Prefix LSA is suppressed, and the component networks remain hidden from other networks.

Default Disabled

Command Mode Router configuration

Usage Guideline The **area range** command is used only with Area Border Routers. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range.

Examples The following example specifies one summary route to be advertised by the Area Border Routers to other areas for IPv6 prefix 2001:0DB8:0:1::/64 and for the Router ID 20.0.1.10.

```
Switch> enable
Switch# configure terminal
Switch(config)# router ipv6 ospf
Switch(config-router)# router-id 20.0.1.10
Switch(config-router)# area 1 range 2001:0DB8:0:1::/64
```

area stub

Use this command to configure an area as a stub area. Use the **no area stub** command to disable this function.

area *AREA-ID* **stub [no-summary]**

no area *AREA-ID* **stub [no-summary]**

Syntax Description	
AREA-ID	Specifies the identifier of the stub area. The identifier can be specified as either an IP address or a decimal value.
no-summary	(Optional) When this option is specified, an ABR will not send summary link advertisements into the stub area.

Default

Stub areas are not configured.

Summary link advertisements are sent into the stub area.

Command Mode

Router configuraiton

Usage Guideline

When employed, this command must be configured on all routers and access servers in the stub area. Use **area default-cost** to specify the cost of the default internal route sent into a stub area by an Area Border Router (ABR).

Two router configuration commands, **area stub** and **area default-cost** are used for stub area router configuration. In all routers attached to the stub area, configure the area using the **area stub** command. Use the **area default-cost** command only for ABRs attached to the stub area.

To prevent advertising LSA summaries into a stub area use the **no-summary** option on ABRs attached to the stub area. The area is defined as a “totally stubby” area using the **area stub no-summary** command on the ABR.

The default summary route (Type 3) will be generated to the stub area (or NSSA area) when **no-summary** is specified in the command.

Example

This command show how to set stub area:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 1 stub
```

Verify the settings by entering the **show ip ospf** command.

area stub (IPv6)

To set the summary-default cost of a stub area, use the area default-cost command. To disable this function, use the no form of this command.

area *AREA-ID* **stub [no-summary]**

no area *AREA-ID* **stub [no-summary]**

Syntax Description	
AREA-ID	Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IPv4 address.
no-summary	(Optional) Prevent an ABR from sending summary link advertisements into the stub area.

Default Disabled

Command Mode Router configuration

Usage Guideline This command is used only on an ABR attached to a stub area. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the **area stub** command. Use the **area default-cost (IPv6) command on page 40** only on an ABR attached to the stub area. The **area default-cost** command provides the metric for the summary default route generated by the ABR into the stub area.

Use the **no-summary** argument with this command to define a totally stubby area. When routers in the area do not require to learn about summary LSAs from other areas, then a totally stubby area should be defined. To define a totally stubby area configure the ABR of that area using the **area stub no-summary** command.

Examples In the following example, the **area stub** command is used to configure the router as a stub that advertises connected and summary routes.

```
Switch > enable
Switch # configure terminal
Switch (config) # router ipv6 ospf
Switch (config-router)# router-id 20.0.1.10
Switch (config-router)# area 1 stub
```

area virtual-link

Use this command to configure a link between two backbone areas that are physically separated through other non-backbone area. Use the **no area virtual-link** command to remove a virtual link.

area *AREA-ID* **virtual-link** *ROUTER-ID* **[authentication [message-digest]] [hello-interval** *SECONDS* **] [dead-interval** *SECONDS* **] [transmit-delay** *SECONDS* **] [retransmit-interval** *SECONDS* **] [[authentication-key** *PASSWORD* **] | [message-digest-key** *KEY-ID* **md5** *KEY* **]]**

no area *AREA-ID* **virtual-link** *ROUTER-ID* **[dead-interval|hello-interval|tansmit-interval|retransmitinterval|authentication|authentication-key|message-digest-key** *KEY-ID***]**

Syntax Description	
AREA-ID	Specifies the identifier of the transit area for the virtual link. The identifier can be specified as either an IP address or a decimal value.
ROUTER-ID	The Router ID of the virtual link neighbor.
authentication	(Optional) Specifies authentication type. If no authentication type is specified for the virtual-link, the authentication type for the area will be used.
message-digest	(Optional) Specifies that message-digest authentication be used.
hello-interval *SECONDS*	Specifies the interval in seconds, between the hello packets that the router sends on an interface. The valid setting is 1-65535.
dead-interval *SECONDS*	Specifies the interval in seconds, during which no packets are received and after which a neighbor is regarded as off-line. The valid setting is 1-65535.
transmit-delay *SECONDS*	The interval the router waits before it transmits a packet. The valid setting is 1-65535.
retransmit-interval *SECONDS*	The interval the router waits before it retransmits a packet. The valid setting is 1-65535.
authentication-key *PASSWORD*	(Optional) Password to be used by neighboring routers. The passsword is a continuous string of keyborad characters up to 8 bytes long. This password is a key to allow the authentication procedure to generate or verify the authentication field contained in the OSPF header. The authentication key is inserted directly into the OSPF header when originating routing protocol packets. Each network can be assigned a separate password on a per-interface basis. All neighboring routers on the same network must use the same password to be able to route OSPF traffic.
message-digest-key *KEY-ID* **md5** *KEY*	(Optional) Key identifier and password to be used for Message Digest 5 (MD5) authentication by neighboring routers and this router. The *KEY-ID* argument is a number in the range from 1 to 255. The *KEY* consists of an alphanumeric string of up to 16 characters in length. All neighboring routers on the same network must have the identical key identifier and key, to be allowed to route OSPF traffic. There is no default value.

Default

- *AREA-ID*: None
- *ROUTER-ID:* None
- **authentication**: null
- **hello-interva**l:10 seconds
- **dead-interva**l: 40 seconds
- **transmit-delay**: 1 second
- **retransmit-interval**: 5 seconds
- **authentication-key:** None
- **message-digest-key**: None

Command Mode

Router configuration

Usage Guideline

In OSPF, all non-backbone areas must be connected to a backbone area. If the connection to the backbone is broken, the virtual link is used to re-establish the connection. Virtual links between any two backbone-routers that have an interface to a common non-backbone area can be configured. The protocol treats these two routers joined by a virtual link as if they were connected by an un-numbered point-to-point network. To configure a virtual link, include both the transit *AREA ID* and the corresponding virtual link neighbor's *ROUTER-ID* in the virtual link neighbor.

Configure the **hello-interval** to be the same for all routers attached to a common network. A short hello interval results in the router detecting topological changes faster but also an increase in the routing traffic.

As with the hello interval, the value of **dead-interval** must be the same for all routers and access servers attached to a common network.

The **retransmit-interval** is the expected round-trip delay between any two routers in a network. Set the value to be greater than the expected round-trip delay to avoid needless retransmissions.

The **transmit-delay** is the time taken to transmit a link state update packet on the interface. Before transmission, the link state advertisements in the update packet, are incremented by this amount. Set the **transmit-delay** to be greater than zero. Also, take into account the transmission and propagation delays for the interface.

Before using the **area virtual-link authentication** command, configure a password for virtual link using the **area virtual-link authentication-key** command. If the **area virtual-link authentication message-digest** command is used, configure the message-digest key for the virtual link using **area virtual-link message-digest-key** command.

The password created by the **area virtual-link authentication-key** command is used as a "key" that is inserted directly into the OSPF header when the switch system software originates routing protocol packets over this virtual link.

Usually, one key per interface (or virtual link) is used to generate authentication information when sending packets and to authenticate incoming packets. The same key identifier on the neighbor router must have the same *KEY* value.

The process of changing keys is as follows. Suppose the current configuration is as follows:

area 1 virtual-link 192.168.255.1 message-digest-key 100 md5 *OLD*

The configuration can be changed to the following:

area 1 virtual-link 192.168.255.1 message-digest-key 101 md5 *NEW*

The system assumes its neighbors do not have the new key yet, so it begins a rollover process. It sends multiple copies of the same packet, each authenticated by different keys. In this example, the system sends out two copies of the same packet; the first one authenticated by key 100 and the second one authenticated by key 101

Rollover allows neighboring routers to continue communication while the network administrator is updating them with the new key. Rollover stops once the local system finds that all its neighbors know the new key. The system detects that a neighbor has the new key when it receives packets from the neighbor authenticated by the new key.

After all neighbors have been updated with the new key, the old key should be removed. In this example, the following entry is used:

no area 1 virtual-link 192.168.255.1 message-digest-key 100

Examples

This following example shows how to establish a virtual link with **hello-interval** and **dead-interval** to 5 and 10 seconds respectively.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 1 virtual-link 10.10.11.50 hello-interval 5
dead-interval 10
```

Verify the settings by entering the **show ip ospf virtual-links** command.

This following example (on the next page) shows how to configure the following parameters for a virtual link at area 1 with the remote id as 192.168.255.1.

1. Specify "yourpass" as the key for simple password authentication.
2. Set authentication type to simple password.

```
Switch# configure terminal
Switch(config)# router ospf 1
Switch(config-router)# area virtual-link 192.168.255.1 authentication-key
yourpass
Switch(config-router)# area 1 virtual-link 192.168.255.1 authentication
```

Verify the settings by entering the **show ip ospf virtual-links** command.

area virtual-link (IPv6)

To define an OSPF virtual link, use the **area virtual-link** command with the optional parameters. To remove a virtual link, use the no form of this command.

area *AREA-ID* **virtual-link** *ROUTER-ID* **[instance-id** *INSTANCE-ID***] [hello-interval** *SECONDS***] [dead-interval** *SECONDS***] [transmit-delay** *SECONDS***] [retransmit-interval** *SECONDS***]**

no area *AREA-ID* **virtual-link** *ROUTER-ID*

Syntax Description	
AREA-ID	Specifies the area ID assigned to the virtual link. This can be either a decimal value or a valid IPv4 address. There is no default.
ROUTER-ID	Specifies the router ID associated with the virtual link neighbor. This can be either a decimal value or a valid IPv4 address. There is no default.
INSTANCE-ID	(Optional) Specifies an Instance identifier. To change this ID from an existing entry, configure the **no area** command first. The valid setting is from 0 to 255.
hello-interval *SECONDS*	(Optional) Specifies the interval in seconds, between the hello packets that the router sends on an interface. The valid setting is 1-65535.
dead-interval *SECONDS*	(Optional) Specifies the interval in seconds, during which no packets are received and after which a neighbor is regarded as off-line. The valid setting is 1-65535.
transmit-delay *SECONDS*	(Optional) The interval the router waits before it transmits a packet. The valid setting is 1-65535.
retransmit-interval *SECONDS*	(Optional) The interval the router waits before it retransmits a packet. The valid setting is 1-65535.

Default No OSPF virtual link is configured.

hello-interval *SECONDS*: 10 seconds

dead-interval SECONDS: 40 seconds

transmit-delay *SECONDS*: 1 second

retransmit-interval *SECONDS*: 5 seconds

Command Mode Router configuration

Usage Guideline All areas in an OSPF autonomous system must be physically connected to the backbone area (area 0). In some cases where this physical connection is not possible, use a virtual link to connect to the backbone through a non-backbone area. As mentioned, use virtual links to connect two parts of a partitioned backbone through a non-backbone area. The area through which the virtual link is configured, is known as a transit area, and it must have the full routing information. The transit area cannot be a stub area.

In OSPF, all non-backbone areas must be connected to a backbone area. If the connection to the backbone is lost, the virtual link repairs the connection. Virtual links can be configured between any two backbone-routers that have an interface to a common non-backbone area. The protocol treats these two routers joined by a virtual link as if they were connected by an un-numbered point-to-point network. To configure a virtual link, include both the transit area ID and the corresponding virtual link neighbor's router ID in the virtual link neighbor.

Configure the **hello-interval** to be the same for all routers attached to a common network. A short hello interval results in the router detecting topological changes faster but also an increase in the routing traffic.

As with the hello interval, the value of **dead-interval** must be the same for all routers and access servers attached to a common network.

The **retransmit-interval** is the expected round-trip delay between any two routers in a network. Set the value to be greater than the expected round-trip delay to avoid needless retransmissions.

The **transmit-delay** is the time taken to transmit a link state update packet on the interface. Before transmission, the link state advertisements in the update packet, are incremented by this amount. Set the **transmit-delay** to be greater than zero. Also, take into account the transmission and propagation delays for the interface.

To configure a virtual link in OSPF for IPv6, a router ID must be used instead of an address. In the IPv6 version of OSPF, the virtual link takes the router ID rather than the IPv6 prefix of the remote router.

Examples

The following example establishes a virtual link with default values for all optional parameters.

```
Switch > enable
Switch # configure terminal
Switch (config) # router ipv6 ospf
Switch (config-router)# area 1 virtual-link 192.168.255.1
```

arp

Use this command to add a static entry in the Address Resolution Protocol (ARP) cache. Use the **no arp** command to remove a static entry in the ARP cache.

arp *IP-ADDRESS HARDWARE-ADDRESS*

no arp *IP-ADDRESS HARDWARE-ADDRESS*

Syntax Description	
IP-ADDRESS	IP address in four-part dotted decimal format corresponding to the local data-link address.
HARDWARE-ADDRESS	Local data-link Media Access (MAC) address (a 48-bit address).

Default No entries are entered in the ARP cache.

Command Mode Global configuration

Usage Guideline Use the **arp** command to assign static and permanent entries to the ARP cache entries. The cache is used to store the IP addresses and the corresponding MAC address so that the addresses will not have to be repeatedly resolved. Static and permanent entries are used for devices that exchange data on a regular basis.

To remove all non-static entries from the ARP cache, use the **clear arp-cache** command.

Example This example shows how to add static ARP entry for a typical Ethernet host:

```
Switch(config)# arp 10.31.7.19 0800.0900.1834
```

Verify the settings by entering the **show arp** command.

arp timeout

Use the **arp timeout** command to set the ARP aging time for the ARP table.

arp timeout *SECONDS*

Syntax Description	
SECONDS	Number of seconds that dynamic entries will remain in the ARP table before being deleted; valid values are from 0 to 65535.

Default 14400 seconds (4 hours)

Command Mode VLAN interface configuration

Usage Guideline Only VLAN interfaces are valid for this command.

Example This example shows how to set the ARP timeout to 12000 seconds to allow entries to time out faster than the default setting:

```
Switch(config)# interface vlan1
Switch(config-if)# arp timeout 12000
```

Verify the settings by using **show ip interface** command

auto-cost reference-bandwidth

Use this command to control how OSPF calculates default metrics for the interface.The no form of this command will reset the reference bandwidth to the default value.

auto-cost reference-bandwidth *MBPS*

no aut-cost reference-bandwidth

Syntax Description	
MBPS	The reference bandwidth in Mbps. The default reference bandwidth is 100 Mbps. The valid setting is 1 to 4294967.

Default Enabled

MBPS: 100

Command Mode Router configuration

Usage Guideline By default OSPF calculates the OSPF metric for an interface by dividing the reference bandwidth by the bandwidth of interface. The default value for the reference bandwidth is 100Mbps. For example, a 100Mbps will have a metric of 1 and a 64K link will have a metric of 1562,

The **auto-cost** command is used to differentiate high bandwidth links. For multiple links with high bandwidth, specify a larger reference bandwidth value to differentiate costs on those links.

Before the cost is changed to the manual configuration mode, the cost must be configured in advance.

Example This following example shows how to set reference bandwidth to 50 Mbps.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# auto-cost reference-bandwidth 50
```

Verify the settings by entering the **show ip protocol ospf** command.

auto-cost reference-bandwidth (IPv6)

To control the reference value IPv6 OSPF uses when calculating metrics for interfaces, use the **auto-cost reference-bandwidth** command. To return the reference value to its default, use the no form of this command.

auto-cost reference-bandwidth *MBPS*

no auto-cost reference-bandwidth

Syntax Description	
MBPS	MBPS Rate in Mbps bandwidth. The range is from 1 to 4294967. The default is 100.

Default *MBPS*: 100.

Command Mode Router configuration

Usage Guideline The IPv6 OSPF metric is calculated as the Mbps value divided by the bandwidth, with Mbps equal to 100 by default, and bandwidth determined by the bandwidth command. The calculation gives Fast Ethernet a metric of 1.

Examples The following example sets the **auto-cost reference bandwidth** to 1000 Mbps.

```
Switch > enable
Switch # configure terminal
Switch (config) # router ipv6 ospf
Switch (config-router)# auto-cost reference-bandwidth 1000
```

banner login

Use banner login to enter the **banner login** mode in order to configure the banner login message. Use the default form of the command to set the login banner to factory default.

banner login *LINE*

default banner login

Syntax Description	
LINE	A displaced string and spaces are allowed. The maximum length is 320 characters. In addition, two special character sequences are used; '/n' is used as new line and '/r ' is used as a carriage return. Please refer to the usage guideline for more detail.

Default

Project dependent

Sample Banner Login Message:

DGS-6604 Chassis Ethernet Switch

Command Line Interface,

Firmware: Build 1.00.027

Copyright (c) 2011 D-Link Corporation, all rights reserved.

Where 2011 represents the year for release of the new firmware. It should be updated if needed by the subsequent release of the firmware.

Command Mode

Global configuration

Usage Guideline

Use this command to define a customized banner to be displayed before the user is prompted for their username and password. Enter the banner login command followed by a desired display string and then execute the command by pressing ENTER to complete the modification.

When a multiple lines banner is needed, use special character sequences such as '/n' which represents a new line and '/r ' which represents a carriage return. However if '/n' or '/r' is required to be displayed as part of the string in the line, then both '/n' and 'r' must be prefixed with another '/' as an escape sequence to overide the special character sequence functionality, for example '//n', or '//r'.

At the end of each line is either a '/n' or '/r' . If more than 80 characters are entered without an '/n' or '/r' ending the line, then the line will be truncated and the first 80 characters are displayed.

Example This example shows how to modify the banner login message:

```
Switch:12(config)# banner login         DGS-6604 Chassis Ethernet Switch
Command Line Interface,
Access for authorized users only. Please enter your username and password.

Switch:12#
```

based-on client-id

This command is used to specify the client identifier as a rule for IP address assignment from the DHCP address pool. Use the no form to remove the rule from DHCP address pool.

based-on client -id {hex|string} *CLIENT-ID*

no based-on client -id {hex|string} *CLIENT-ID*

Syntax Description	
CLIENT-ID	A sequence of bytes or a string defined on the client that is an unique identification of client. HEXADECIMAL: The maximum length is 128 bytes. STRING: The maximum length is up to 64 bytes.

Default None

Command Mode DHCP pool configuration

Usage Guideline All rules take effect on the corresponding DHCP address pool and will have a logical AND operation conditions combined with other rules set by other based-on commands.

If a DHCP client sends the no DHCP Client Identifier option, the service continues to operate as it bases it on the hardware type and a client hardware address. If a DHCP client sends a DHCP Client Identifier option, the DHCP server validates the value to ensure the client identifer optional field matches the configured Client Identifier. If the values match, the DHCP server provides service to the client. If the values do not match, the DHCP server does not respond to the client's request.

Multiple based-on client-id commands create a list of client-ids for the DHCP address pool. When any request has a match in the list, the server will provide an IP address to the server based on DHCP Client Identifier option, but not the received client Hardware address.

Examples The following sets a rule used for the IP address assignment based 0x0152415320 for a Microsoft "Remote Access Server" (RAS).

```
switch(config)#ip dhcp pool pool1
switch(config-dhcp)#based-on client-id hex 0x0152415320
```

based-on c-vid

This command is used to specify the customer vlan ID (C-VID) as a rule for IP address assignment from the DHCP address pool. Use the no form of the command to remove the C-VID rule from DHCP address pool.

based-on c-vid *V-ID* **[,|-]**

no based-on c-vid *V-ID* **[,|-]**

Syntax Description	
V-ID **[,|-]**	Specifies the V-ID list.

Default None

Command Mode DHCP pool configuration

Usage Guideline This command is used to create the address binding rule for the DHCP address pool. The **based-on c-vid** command creates the address binding rules in an incremental way. That is, all of the C-VIDs created by **based-on c-vid** commands take effect on the corresponding DHCP address pool. However this command will be combined with logical AND operations with the other rules set by other **based-on** commands. For example if the first rule is **based-on c-vid** *100* and there is another **based-on s-vid** *200* command, then the address pool will only assign an IP address to the client with C-VID=100 and S-VID=200.

Examples The following sets a rule used for IP address assignment based on C-VID 100 or 200 from the DHCP address pool1.

```
switch(config)#ip dhcp pool pool1
switch(config-dhcp)#based-on c-vid 100,200
```

Then the rule is added to and now based on C-VID 100/ 200 and S-VID 1000.

```
switch(config-dhcp)#based-on s-vid 1000
```

based-on interface-ip-address

This command is used to specify a rule for a DHCP address pool to respond to a request from the specified IP interface. Use the no form of the command to remove the rule from the DHCP address pool.

based-on interface-ip-address *IP-ADDRESS*

no based-on interface-ip-address *IP-ADDRESS*

Syntax Description	
IP-ADDRESS	Specifies the IP address of the interface.

Default None

Command Mode DHCP pool configuration

Usage Guideline An additional rule can be set for a DHCP address pool based on interface IP address.

All of the DHCP IP address assignment rules take effect on the corresponding DHCP address pool. A based-on command will be combined using logical AND operations with the other rules set by all other based-on commands.

Examples The following example sets a rule used for the IP address assignment (DHCP IP address pool1) based on interface 172.19.10.100.

```
switch(config)#ip dhcp pool pool1
switch(config-dhcp)#based-on interface-ip-address 172.19.10.100
```

based-on mac-address

This command is used to specify the host MAC address as a rule for IP address assignment from the DHCP address pool. Use the no form to remove the MAC address rule from the DHCP address pool.

based-on mac-address *MAC-ADDRESS* **[,|-]**

no based-on mac-address *MAC-ADDRESS* **[,|-]**

Syntax Description	
MAC-ADDRESS **[,|-]**	Specifies the MAC address list.

Default None

Command Mode DHCP pool configuration

Usage Guideline This command is used to create the address binding rule for the DHCP address pool. **based-on mac-address** command creates the address binding rules in an incremental way. That is, all of the mac-addresses created by the based-on mac-address commands take effect on the corresponding DHCP address pool. However this command will be combined using logical AND operations with the other rules is set by all other based-on commands. For example if the first rule is **based-on mac-address** *00:80:00:11:22:00- 00:80:00:11:22:FF* and there is another **based-on c-vid** *200* command, the address pool will only assign an IP address to the client with a MAC address in range of 00:80:11:22:xx and with its C-VID=200. Other than that, no IP address is offered from the corresponding DHCP address pool.

Examples The following sets a rule used for IP address assignment based on MAC address 00:80:C8:11:22:xx from the DHCP address pool1.

```
switch(config)#ip dhcp pool pool1
switch(config-dhcp)#based-on mac-address 00:80:C8:11:22:00-00:80:C8:11:22:FF
```

The following sets an additional rule used for IP address assignment based on MAC address 00:80:C8:11:33:00 and 00:80:C8:11:33:FF from the DHCP address pool1.

```
switch(config-dhcp)#based-on mac-address 00:80:C8:11:33:00,00:80:C8:11:33:FF
```

based-on relay-ip-address

This command is used to specify a rule for the DHCP address pool's only response for BOOTP forwarder or relay. Use the no form of the command to remove the rule from a DHCP address pool.

based-on relay-ip-address *IP-ADDRESS*

no based-on relay-ip-address *IP-ADDRESS*

Syntax Description	
IP-ADDRESS	Specifies the IP address of BOOTP forwarder for relay.

Default None

Command Mode DHCP pool configuration

Usage Guideline An additional rule can be set for DHCP address pool for each relay IP address.

All of the DHCP IP address assignment rules take effect to the corresponding DHCP address pool. All of the based-on commands will be combined using logical AND operations with other rules set by all the other based-on commands.

Examples The following example sets a rule used for IP address assignment (DHCP IP address pool1) based on the Relay IP address.

```
switch(config)#ip dhcp pool pool1
switch(config-dhcp)#based-on relay-ip-address 10.1.1.254
```

based-on s-vid

This command is used to specify the service provider vlan ID (S-VID) as a rule for IP address assignment from the DHCP address pool. Use the no form of the command to remove the S-VID rule from the DHCP address pool.

based-on s-vid *V-ID* **[,|-]**

no based-on s-vid *V-ID* **[,|-]**

Syntax Description	
V-ID **[,|-]**	Specifies the V-ID list.

Default None

Command Mode DHCP pool configuration

Usage Guideline This command is used to create the address binding rule for the DHCP address pool. The **based-on s-vid** command creates the address binding rules in an incremental way. That is, all of S-VID created by based-on s-vid commands take effect on the corresponding DHCP address pools. However this command will be combined using logical AND operations with the other rules set by other based-on commands. For example if the first rule is **based-on s-vid** *100* and there is another **based-on c-vid** *200* command, then the address pool will only assign an IP address to the client with C-VID=200 and S-VID=100.

Examples The following sets a rule used for IP address assignment based on S-VID 100 or 200 from the DHCP address pool1.

```
switch(config)#ip dhcp pool pool1
switch(config-dhcp)#based-on s-vid 100,200
```

Below the rule becomes based on S-VID 100/ 200 and C-VID 1000.

```
switch(config-dhcp)#based-on c-vid 1000
```

based-on user-class

This command is used so that DHCP administrators can define specific user class identifiers to convey information about a client's software configuration or about its user's preferences. Use the no form of the command to remove the related setting rule.

based-on user-class {hex *HEXADECIMAL* **|string** *STRING***}**

no based-on user-class {hex *HEXADECIMAL* **|string** *STRING***}**

Syntax Description	
HEXADECIMAL	A leading string, 0x has to indicated and then a following hexadecimal sequence must be entered. The maximum length is 128 bytes.
STRING	Displayable string but no spaces are allowed. The maximum length is up to 64 bytes.

Default None

Command Mode DHCP pool configuration

Usage Guideline This command is used to create the address binding rule for the DHCP address pool. One user class is allowed in one DHCP address pool. Use the no form of the command to remove user-class rule.

This command will be combined using logical AND operations with the other rules set by all the other based-on commands. For example, if the first rule is **based-on user-class** *alpha* and there is another **based-on c-vid** *200* command, the address pool will only assign an IP address to the client which has C-VID=200 and user class as *alpha*.

Examples The following sets a rule used for IP address assignment based on the user class *alpha* from DHCP address pool1.

```
switch(config)#ip dhcp pool pool1
switch(config-dhcp)#based-on user-class string alpha
```

The following sets a rule used for IP address assignment based on the user class 0x8080 from DHCP address pool1.

```
switch(config)#ip dhcp pool pool1
switch(config-dhcp)#based-on user-class hex 0x8080
```

based-on vendor-class

This command is used to create an address binding rule for the DHCP address pool based on the vendor class. Use the no form of the command to delete the related rule setting.

based-on vendor-class {hex *HEXADECIMAL* **|string** *STRING***}**

no based-on vendor-class {hex *HEXADECIMAL* **|string** *STRING***}**

Syntax Description	
HEXADECIMAL	A leading string, 0x has to be entered and then a following hexadecimal sequence must be entered. The maximum length is 128 bytes.
STRING	A displayable string with no spaces allowed. The maximum length is up to 64 bytes.

Default None

Command Mode DHCP pool configuration

Usage Guideline This command is used to create the address binding rule for the DHCP address pool. One vendor class is allowed in one DHCP address pool. Use the no form of the command to remove the user-class rule.

For vendor classes, e.g. DHCP-requests from Windows 98SE/ME are sent with a vendor class of MSFT 98 and from Windows 2000/XP with a vendor class of MSFT 5.0. The received VendorClass-ID string is compared with the specified string. If the received string is longer than the specified string, then the excess characters are ignored. For example, specifying MSFT will match both Win98SE/ME and 2000/XP.

This command will be combined using logical AND operations with the other rules set by all the other based-on commands. For example if the first rule is **based-on vendor-class string** *MSFT 5.0* and there is another **based-on c-vid** *200* command, the address pool only assigns an IP address to the client which has C-VID=200 and its vendor class set to MSFT 5.0.

Examples The following example sets the vendor class to match both Win98SE/ME and 2000/XP.

```
switch(config)#ip dhcp pool pool1
switch(config-dhcp)#based-on vendor-class string MSFT
```

bgp always-compare-med

Use this command to compare the Multi-Exit Discriminator (MED) for paths from neighbors in different autonomous systems. Use the **no bgp always-compare-med** command to disallow the comparison.

bgp always-compare-med

no bgp always-compare-med

Syntax None

Default Disabled

Command Mode Router configuration

Usage Guideline The MED, as stated in RFC 1771, is an optional nontransitive 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 is 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 comparisons between all paths, regardless of the autonomous system from which the paths are received.

The **bgp deterministic-med command on page 75** can be configured to enforce a deterministic comparison of the MED value between all paths received from within the same autonomous system.

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

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

bgp asnotation dot

Use this command to change the default display and regular expression match format of BGP 4-byte AS numbers from asplain (decimal values) to dot notation. Use the no form of the command to reset the default 4-byte autonomous system number display and regular expression match format to asplain.

bgp asnotation dot

no bgp asnotation dot

Syntax None

Default BGP AS numbers are displayed using asplain (decimal value) format in screen output, and the default format for matching 4-byte autonomous system numbers in regular expressions is asplain.

Command Mode Router configuration

Usage Guideline BGP AS numbers that were allocated to companies were 2-byte numbers in the range from 1 to 65535 as described in RFC 4271. Due to increased demand for AS numbers, the IANA will start, in January 2009, to allocate four-byte AS numbers in the range from 65536 to 4294967295. RFC 5396 documents three methods of representing autonomous system numbers. BGP has implemented the following two methods:

- **Asplain-Decima**l value notation where both 2-byte and 4-byte AS numbers are represented by their decimal value. For example, 65525 is a 2-byte AS number and 65545 is a 4-byte autonomous system number.

- **Asdot-Autonomous** system dot notation where 2-byte AS numbers are represented by their decimal value and 4-byte AS numbers are represented by a dot notation. For example, 65525 is a 2-byte autonomous system number and 1.10 is a 4-byte AS number (this is dot notation for the 65545 decimal number).

After the command is performed, the output is converted in order to format it. For some of the information which is learned prior, for example: *routes*, the AS notation format follows the previous format. Therefore, the **clear ip bgp command on page 94** must be used to convert to the current format.

Example This example (on the next page) shows how to configure asnotation and shows the difference using the command **show ip bgp**:

```
Switch # show ip bgp
BGP table version is 30, local router ID is 10.10.11.50
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.0.1.0/24     10.10.71.100             0             0 65636 i
*> 192.0.2.0/24     10.10.71.100             0             0 65636 {80} i

Total Entries: 2 entries, 2 routes
Switch #config terminal
Switch(config)# router bgp 1.6553465636
Switch(config-router)# bgp asnotation dot
Switch(config-router)# end
Switch # clear ip bgp *
Switch # show ip bgp
BGP table version is 30, local router ID is 10.10.11.50
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.0.1.0/24     10.10.71.100             0             0 1.101  100  i
*> 192.0.2.0/24     10.10.71.100             0             0 1.101 100 {80} i

Total Entries: 2 entries, 2 routes
Switch #
```

bgp bestpath as-path ignore

Use this command to ignore AS path as a factor in the selection of the best path. Use the no form of the command to restore the 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 in the best path selection.

Command Mode Router configuration

Usage Guideline The following are the rules used for the best path selection process.

1. If the next hop associated with the route is unreachable, then the route is 1. If the next hop associated with the route is unreachable, then the route is dropped.
2. The next choice is the route with the largest weight is selected.
3. If weight cannot make the determination, then the largest LOCAL_PREF is used to determine the preferred route.
4. If the preferred route can still not be determined, then the route with the shortest AS_PATH list is preferred.
5. If the preferred route can still not be determined, then lowest origin type is preferred.
6. If the preferred route can still not be determined, then the lowest MED is preferred.
7. If the preferred route can still not be determined, then eBGP is preferred over iBGP paths.
8. Always prefer the path with the lowest IGP metric to the BGP next hop.
9. Check to determine if multiple paths require installation in the routing table for BGP Multipath.
10. When both paths are external, always prefer the path that was received first (the oldest one).
11. Always 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. Always prefer the path that comes from the lowest neighbor address.

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

Example

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

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

bgp bestpath compare-routerid

Use this command to compare router IDs for the best-path selection process when external BGP (eBGP) paths are identical. Use the no form of the command 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

Usage Guideline When comparing similar routes from peers the BGP router does not consider the router ID of the routes. By default, it selects the first received route. Use this command to include the router ID in the selection process. When enabled, similar routes are compared and the route with the lowest router ID is selected. Unless manually defined, 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 on page 78**.

Example This example shows how to configure to compare the router-ids of identical eBGP paths for autonomous system 65534:

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

bgp default ipv4-unicast

Use this command to enable the IP version 4 (IPv4) unicast address family for all neighbors. This affects the BGP global configuration. Use the no form of the command to disable this function.

bgp default ipv4-unicast

no bgp default ipv4-unicast

Syntax None

Default **bgp default ipv4-unicast**

Command Mode Router configuration

Usage Guideline The **bgp default ipv4-unicast** command is used to enable the automatic exchange of IPv4 address family prefixes.

Example This example shows how to configure BGP defaults and activate **ipv4-unicast** of a peer by default for autonomous system 65534:

```
Switch(config)# router bgp 65534
Switch(config-router)# bgp default ipv4-unicast
```

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 preference is 0 to 4294967295. A higher number is prefered to a lower number in the comparison.

Default *NUMBER*: 100

Command Mode Router configuration.

Usage Guideline The local preference attribute is a discretionary attribute that is used to apply a degree of preference to a route during the BGP best path selection process.

This attribute is exchanged only between iBGP peers and used to determine local policy. The route with the highest local preference becomes the preferred route.

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

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

Verify the settings by entering **show ip protocols bgp** command.

bgp deterministic-med

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

bgp deterministic-med

no bgp deterministic-med

Syntax None

Default The default value is disabled.

Command Mode Router configuration

Usage Guideline The **bgp always-compare-med command on page 67** is used to enable the comparison of the MED value for paths from neighbors in different autonomous systems. After the **bgp always-compare-med** is enabled, all paths for the same prefix that are received from different neighbors 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 then picks the best paths using the existing rules; the comparison is first made on a per neighbor autonomous system basis and then on a 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 is used to enforce deterministic comparison of the MED value between all paths received from within the same autonomous system. When enabled, the result of the selection algorithm is the same regardless of the order in which the paths are received on the local router.

Example This example shows how to configure to enable comparison of MED values for autonomous system 65534:

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

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 None

Default Disabled

Command Mode Router configuration.

Usage Guideline This command specifies that any updates received from an external neighbor that do not have the neighbor's configured Autonomous System (AS), at the beginning of the AS path, 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.

Example 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 is the local AS number of the transmitting peer:

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

bgp log-neighbor-changes

Use the **bgp log-neighbor-changes** command to enable logging of BGP neighbor resets. Use **no bgp log-neighbor-changes** to disable the logging.

bgp log-neighbor-changes

no bgp log-neighbor-changes

Syntax None

Default Disabled.

Command Mode Router configuration.

Usage Guideline This command enables logging of both BGP resets and alternating status changes to use for toubleshooting purposes .

Unexpected neighbor resets might indicate high error rates or high packet loss in the network and should be investigated.

The neighbor status change messages are not tracked if the bgp log-neighbor-changes command is not enabled. The exception to this is for a reset reason, which is always available as output of the s**how ip bgp neighbors** and **show bgp ipv6 neighbors** commands.

The logs for BGP neighbor changes will display on the console.

Example This example shows how to enable logging of BGP neighbor changes for autonomous system 65534:

```
Switch(config)# router bgp 65534
Switch(config-router)# bgp log-neighbor-changes
```

Use the **show logging buffer** command to display the log for the BGP neighbor changes.

bgp router-id

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

bgp router-id *IP-ADDRESS*

no bgp router-id [*IP-ADDRESS***]**

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

Default The router ID is set to the highest IP address on a physical interface.

Command Mode Router configuration

Address family configuration

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

The router ID specified must be unique within the network. This command resets all active BGP peering sessions.

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

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

boot config

Use this command to specify the file that will be used as the configuration file for the next boot up.

boot config [check] *MEDIUM: URL*

no boot config

Syntax Description	
MEDIUM:URL	Specifies the media where the file system is located. The valid values are flash:\, cf1:\., etc. flash:\ represents system internal on-board FLASH memory. cf1:\ represents the first (left) open slot compact FLASH memory. URL - Specifies the file to be assigned.
check	(Optional) This option is used for show the configuration file information for the specified file. The information includes the file and model names.

Default Default configuration file is def_usr.conf

Command Mode Global configuration

Usage Guideline The **boot config** command specifes the file system and file name of the configuration file to use for initialization (startup). The configuration file must be an ASCII file located in the specified file system.

The command takes affect immediately and will be kept in NVRAM.

In the following situations the boot configuration does not update and an error message is displayed:

- A configuration file is specified where the filename argument does not exist or is not valid causing the boot configuration to not update and an error message to be displayed.
- During initialization, the factory default configuration is used when the boot config setting does not exist or when it is null (such as at a first-time start-up). If the software detects a problem with the boot config file, the device uses the factory default configuration for system boot up.
- When using the no form of this command, the boot configuration resets to the default configuration

Use the **show boot** command to view the contents of the **boot config** configuration file.

Initially, a system file is used as the factory default configuration.

The specified URL must be represented by an absolute path. It cannot be represented by a relative path.

Examples

The following example shows how to specify the file *switch-config* as the startup configuration file:

```
Switch# configure terminal
Switch(config)# boot config flash:\switch-config
Switch(config)# end
```

Verify the settings by entering the **show boot** command.

The following example shows the result of specifying the incorrectly formed file *yyy-config* as the startup configuration file.

```
Switch# configure terminal
Switch(config)# boot config flash:\yyy-config.exe
Illegal configuration file
Switch(config)# end
```

bootfile

This command is used to specify the name of the default boot image for a Dynamic Host Configuration Protocol (DHCP) client. To delete the boot image name, use the no form of the command.

boofile *URL*

no bootfile

Syntax Description	
URL	Specifies the path name and file name of the file that is used as a boot image. The maximum allowed string length is 127 characters

Default None

Command Mode DHCP pool configuration

Usage Guideline Use this command to specify the name of the default boot image for a Dynamic Host Configuration Protocol (DHCP) client. The boot image can be located in the same DHCP server or other network servers.

Examples The following example specifies *mdubootfile* as the name of the boot file for DHCP pool1.

```
switch > enable
switch# configure terminal
switch(config)# ip dhcp pool pool1
switch(config-dhcp)# bootfile \dgs-6600\bootimage\mdubootfile.bin
switch(config-dhcp)#
```

boot image

Use this command to specify the file used as the image file for the next boot.

boot image [check] *MEDIUM: URL*

Syntax Description	
MEDIUM	Specifies the media where the file system is located. The valid values are flash:\ and cf1:\. Flash:\ represents the on-board FLASH storage of the active control module. cf1:\ represents the first opened slot compact FLASH storage. URL: Specifies the file to be assigned.
check	(Optional) This option is used to show the firmware information for the specified file. The information includes file name, model name, version number, checksum, time stamp (if any).

Default None

Command Mode Global configuration

Usage Guideline This command is only available at privilege level 15.

The **boot image** command specifies the boot image file to be used for the next start up. Upon start up, the previous boot image becomes the secondary boot up image file.

There can be up to three boot image files in the list with the secondary position and tertiary position used as backup boot image files in sequence.

When this command is used to assign a file as the next-boot image file, the system will check the checksum and model to determine whether the file is a correct image file.

The specified URL must be represented by the absolute path. It cannot be represented by the relative path. Spaces are not allowed in either directory or file names of the absolute path as they will cause load failure of the boot image.

The **check** keyword option allows the user to check a new image file format to verify whether it is suitable to be a boot image or not. The option verfies and displays information such as the file name/content, version number, time stamp (it any), checksum, file size, etc.. The check option compares the information with that in the current boot image file.

If the storage media for the specified URL (filename) does not exist, an error message is displayed with the notification of the URL error.

Examples The following example (on the next page) shows how to specify the switch to use the image file named switch-image1.bin as the boot image file for the next startup and the previous boot image,flash:\switch-image0.bin becomes the secondary boot image file in the list and changes the status to the backup boot image.

```
Switch# configure terminal
Switch(config)#boot image flash:\images\switch_image1.had
Checking image at local flash:\images\switch_image1.had ...  Done.
Update bootlist ....... Done.

Success
```

Verify the settings by entering the **show boot** command.

channel-group

Use the **channel-group** command to assign an interface to a channel group. Use **no channel-group** to remove an interface from a channel-group.

channel-group *CHANNEL-NO* **mode { on| active| passive }**

no channel-group

Syntax Description	
CHANNEL-NO	Specifies the Channel group ID.
mode { on | active | passive }	Specifies the mode of channel group as follows: • on - The interface is the static member of the channel-group. • active - The interface is to operate in LACP active mode. • passive - The interface is to operate in LACP passive mode.

Default None

Command Mode Interface configuration

Usage Guideline The system automatically creates the port-channel when the channel group gets its first physical port.

An interface can be in one mode only and in one channel-group only.

If the mode **on** is specified in the command, the channel group is of a static type. If the mode **active** or **passive** is specified in the command, the channel group is LACP type. A channel group can only have either static member or dynamic members. That is, once the type of a channel group is determined, interfaces in other types cannot join the channel group.

Only a physical port interface is allowed to specify the channel-group. The **no** command removes the interface from the channel group. If the channel group has no member port left after removal, it is deleted automatically.

Configuration of a channel group has the following limitations:

- If dot1x, port security, IP-MAC-Port binding, MAC AC or WAC are enabled for a port, the port cannot be specified as a channel group member.
- In order to be a member of the LACP channel-group, the port must be set to full duplex. LACP will not prevent the user configuration of the port whether it is set to full duplex or not and if these ports have various duplex setting in the same channel group. LACP protocol behavior will choose the members that are set to full duplex for the link aggregation.

- In order to be a member of the LACP channel-group, the member ports must have the same speed setting. LACP will not prevent the user configuration if these ports have difference speed setting in the same channel group. LACP protocol behavior will choose the members that have the same speed to for the link aggregation.

Example

This example shows how to configure a channel group. It assigns the eth3.4 to 3.5 to port-channel 3 with the LACP mode active.

```
Switch(config)# interface range  eth3.4-3.5
Switch(config-if)# channel-group 3 mode active
```

Verify the settings by entering the **show channel-group** command

class

Use this command to specify the name of the class map in order to define its traffic policy and enter into *policy-map class* configuration mode. Use the no form of the command to remove the policy definition for the specified class. All the traffic that does not match any defined class will be classified to default class, class-default.

class *NAME*

no class *NAME*

class class-default

Syntax Description	
NAME	Specifies the name of the class map that the class policy. Up to 32 characters are allowed.

Default None

Command Mode Policy-map configuration

Usage Guideline The class map needs to be created before the policy can be configured for it. A class-map without any match commands cannot be configured as a class policy.

This command enters the *policy-map class* configuration mode. The user can use the set command and police command to define the QoS policy for the class.

class-default is the reserved name for the default class. All the traffic that does not match any defined class will be classified to **class-default**.

Examples This example shows how to define a policy map, policy1 which defines policies for class, class-dscp-red. The packet that matches DSCP 10, 12, or 14 will be set to new DSCP 10 and policed by a single rate policer.

```
Switch(config)# class-map class-dscp-red
Switch(config-cmap)# match ip dscp 10,12,14
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class class-dscp-red
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)# police 64 128 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

Verify the settings by entering the **show policy-map** command.

class-map

To create a class map to be used for matching packets to a specified class, use the **class-map** command. To remove an existing class map from the switch, use the no form of this command. The **class-map** command enters the *class-map* configuration mode in which multiple issues of the **match command on page 405** can be entered to configure the match criteria for this class.

class-map [match-any] *NAME*

no class-map *NAME*

Syntax Description	
NAME	Name of the class for the class map. The name can be a maximum of 32 alphanumeric characters. The class name will be referenced in policy map to configure the policy for the class.
match-any	(Optional) Determines how to evaluate the multiple match criteria. Match statements in this class map will be evaluated based on the logical “OR” function.

Default

Only the class-default exists by default.

All traffic that does not match any defined class will be classified to class-default.

Command Mode

Global configuration

Usage Guideline

Use the **class-map** command to specify the class that will create or modify the match criteria. This command enters *class-map* configuration mode where **match** commands are entered to configure the match criteria for this class. Packets that arrive at the ingress port are checked against the match criteria for a class map to determine if the packets belong to that class.

When configuring a class map, use one or more **match** commands to specify multiple match criteria. For example, use the **match access-list** command, the **match protocol** command, the **match vlan** command, the **match dscp** command, the **match precedence** command or the **match cos** command.

When configuring multiple **match** commands for a class, use the **match-any** keyword to specify whether to evaluate the multiple match criteria based on using logical OR.

A maximum of 256 class maps are allowed.

The name *class-default* is reserved.

Example

The following example (on the next page) specifies class_home_user as the name of a class map. In this class map, a match statement specifies that the

traffic that matches the access control list acl_home_user or match ipv6 protocol will be included in class_home_user.

```
Switch(config)# class-map match-any class_home_user
Switch(config-cmap)# match access-list acl_home_user
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch(config)#
```

Verify the settings by entering the **show class-map** command.

clear arp-cache

To remove dynamically created entries from the Address Resolution Protocol (ARP) cache, use the **clear arp-cache** command in Privileged EXEC mode.

clear arp-cache [interface *INTERFACE-ID* | *IP-ADDRESS*]

Syntax Description	
INTERFACE-ID	(Optional) Removes only the ARP table entries associated with this interface such as for example, vlan100 for the VLAN interface.
IP-ADDRESS	(Optional) IP address to clear from the ARP table.

Default None

Command Mode Privileged EXEC

Usage Guideline This command is used to delete dynamic entries from the ARP cache. The user can select to delete all dynamic entries, specific dynamic entries, or dynamic entries that are associated with a specific IP interface.

Example This example shows how to removes all dynamic entries from the ARP cache.

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

clear counters

Use the command to clear counters for a specific port interface or all port interfaces.

clear counters [*INTERFACE-ID* **[, | -]]**

Syntax Description	
INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, all counters on applicable interfaces (physical ports) will be cleared.

Default None

Command Mode Privileged EXEC

Usage Guideline For now, only physical port counters are provided.

Examples This example shows how to clear counters of interface eth3.10.

```
Switch# clear counters eth3.10
Switch#
```

The following example will clear all of physical ports' statistic counters.

```
Switch# clear counters
Switch#
```

The following example will clear eth 3.1-3.24 physical port s' statistic counters.

```
Switch# clear counters eth3.1-3.24
Switch#
```

clear dos prevention counter

Use this command to clear the counter of all attack types.

clear dos_prevention counter

Syntax None

Default None

Command Mode Global configuration.

Usage Guideline Use to reset counters of DoS prevention to zero.

Examples This example shows how to clear counters.

```
Switch(config)# clear dos_prevention counter
Switch(config)#
```

Below is an example of using the **show dos_prevention** command to display the DoS frame counts:

```
Switch(config)#show dos_prevention
DoS Prevention Information
 Action: Drop
 Frame Counts: 242

 DoS Type                                        State
-------------------------------------------------------
Land Attack                                  Enabled
Blat Attack                                  Enabled
Smurf Attack                                 Enabled
TCP Null                                     Enabled
TCP Xmas                                     Enabled
TCP SYNFIN                                   Enabled
TCP SYN SrcPort Less Than 1024               Enabled
```

clear cpu-protect counters

Use this command to clear the cpu-protect related counters.

clear cpu-protect counters [sub-interface [manage | protocol | route] | type [*PROTOCOL-NAME***]]**

Syntax Description	
sub-interface [manage | protocol | route]	(Option) Clear the cpu-protect related counters of all sub-interfaces if no sub-interface name is specified. Specify the sub-interface name to clear the counter of the specific sub-interface.
type [*PROTOCOL-NAME***]**	(Optional) Clear the cpu-protect related counters of all protocols if no protocol name (for example, **bgp**) is specified. Specify the protocol name to clear specific counter. See the “Usage Guideline” of the command **cpu-protect type** for the valid protocol string.

Default None

Command Mode Privileged EXEC mode

Usage Guideline If the command **clear cpu-protect** counters is issued without option, all cpu-protect related counters will be cleared.

Example The following example shows how to clear all cpu-protect related statistics.

```
Switch# clear cpu-protect counters
```

clear gvrp statistics interface

Use the **clear gvrp statistics** command to clear the statistics of a single port, a range of ports or all gvrp ports.

clear gvrp statistics [interface *INTERFACE-ID* **[, | -]]**

Syntax Description	
INTERFACE-ID	(Optional) Specifies the interface to be cleared. If no interface is specified the statistics on all interfaces will be cleared.
,	(Optional) Specifies a series of interfaces, or separates a range of interfaces from a previous range.
-	(Optional) Specifies a range of interfaces.

Default None

Command Mode Privileged EXEC mode

Usage Guideline This command clears the GVRP counters. If the interface-ID is not specified all GVRP counters for all interfaces will be cleared.

Example This example shows how to clear the GVRP statistics on all interfaces.

```
Switch# clear gvrp statistics
Switch#
```

clear ip bgp

To reset BGP connections using hard or soft reconfiguration, use the **clear ip bgp** command.

clear ip bgp { * | *AUTONOMOUS-SYSTEM-NUMBER* **|** *NEIGHBOR-ADDRESS***} [soft] [in | out]**

Syntax Description	
*****	Specifies that all current BGP sessions will be reset.
AUTONOMOUS-SYSTEM-NUMBER	Specifies that sessions with BGP peers in the specified autonomous system will be reset.
NEIGHBOR-ADDRESS	Specifies that the session of the identified BGP neighbor will be reset. The value for this argument can be an IPv4 or IPv6 address.
in	(Optional) Initiates inbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
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 reset the session.

Default None

Command Mode Privileged EXEC

Usage Guideline Use of the **clear ip bgp** command allows a reset of the neighbor sessions with varying degrees of severity, depending on the specified keywords and arguments.

Use the * keyword to reset all neighbor sessions. The software will clear and then reset the neighbor connections. Use this form of the command in the following situations:

- Modifying the BGP timer specification
- Modifying the BGP administrative distances

Use the **soft** and **out** keywords to clear and reset only the outbound neighbor connections. Inbound neighbor sessions will not be reset. Use this form of the command in the following situations:

- Additions or modifications are made to the BGP-related access lists
- Modifying the BGP-related weights
- Modifying the BGP-related distribution lists
- Modifying the BGP-related route maps

Use the **in** keyword to clear only the inbound neighbor connections. Outbound neighbor sessions will not be reset. Use this form of the command in the following situations:

- Additions or modifications to BGP-related access lists.
- Modifying the BGP-related weights
- Modifying the BGP-related distribution lists
- Modifying the BGP-related route maps

If inbound routing tables are reset, all BGP routers must support route refresh capability (RFC 2918).

Example

In the following example, the BGP session is reset for BGP neighbor 172.5.78.12:

```
Switch# clear ip bgp 172.5.78.12
Switch#
```

clear ip bgp peer-group

To reset BGP connections using hard or soft reconfiguration for all the members of a BGP peer group, use the **clear ip bgp peer-group** command.

Without Address Family Syntax

clear ip bgp peer-group *PEER-GROUP-NAME* **[soft] [in | out]**

Syntax Description	
PEER-GROUP-NAME	Peer group name.
in	(Optional) Initiates inbound reconfiguration. If neither the **in** nor **out** keywords are specified, both inbound and outbound sessions are reset.
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 EXEC

Usage Guideline The **clear ip bgp peer-group** command is used to initiate a hard reset or soft reconfiguration for neighbor sessions of BGP peer groups. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions.

Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow application of a new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Use this command whenever any of the following changes occur:

- Additions or modifications to the BGP-related access lists
- Modifications to BGP-related weights
- Modifications to BGP-related distribution lists
- Modifications to BGP-related route maps

The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for nondisruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh is advertised through BGP capability negotiation. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors command on page 600** command. The following message is displayed in the output when the router supports the route refresh capability:

Received route refresh capability from peer

If all BGP routers support the route refresh capability, use the **clear ip bgp peer-group** command with the **in** keyword. It is not necessary to use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.

Examples

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 the inbound session with members of the peer group INTERNAL, and the outbound session is unaffected:

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

clear ip dhcp binding

Use this command to delete an address binding from the DHCP Server database.

clear ip dhcp binding [pool *NAME***] [***ADDRESS***]**

Syntax Description	
pool *NAME*	(Optional) Name of the DHCP pool. If the pool name option is not specified the command will parse all the DHCP pools for the specified binding.
ADDRESS	(Optional) The IP address of binding to be deleted. If no address is specified, all of bound addresses are cleared.

Default None

Command Mode Privileged EXEC

Usage Guideline Use this command to delete the address of the binding. The address denotes the assigned client's IP address. If no IP address is specified, DHCP server clears all bindings.

Note the following behavior for the **clear ip dhcp binding** command:

- If the pool *NAME* option is not specified and an IP *ADDRESS* is specified, it is assumed that the IP address is an address in the global address space and the command will parse all the DHCP pools for the specified binding.
- If both the pool *NAME* option and the *ADDRESS* option are not specified, it is assumed that all bindings in all pools are to be deleted.
- If the pool *NAME* option is specified without the ADDRESS option being specified, then all the bindings in the specified pool will only be cleared.
- If the pool *NAME* option and an IP *ADDRESS* is specified, the specified binding will be deleted from the specified pool.

Examples The following example deletes the address binding 10.12.1.99 from DHCP server database:

```
swtich# clear ip dhcp binding 10.12.1.99
swtich#
```

The following example deletes all bindings from all pools:

```
switch# clear ip dhcp binding
```

The following example deletes address binding 10.13.2.99 from the address pool named pool2:

```
switch# clear ip dhcp pool pool2 binding 10.13.2.99
switch#
```

Verify the settings by entering the **show ip dhcp binding** command.

clear ip dhcp conflict

Use this command to clear an address conflict from the DHCP server database.

clear ip dhcp conflict [pool *NAME***] [***ADDRESS***]**

Syntax Description	
pool *NAME*	(Optional) Name of the DHCP pool.
ADDRESS	(Optional) The IP address, that is in conflict, to be deleted

Default None

Command Mode Privileged EXEC

Usage Guideline Use this command to delete the address in conflict. The DHCP server detects the conflict of an IP address by using a ping session. If no IP address is specified, DHCP server clears all known IP addresses that are in conflict.

The server detects conflicts using a ping session. The client detects conflicts using gratuitous Address Resolution Protocol (ARP).

Note the following behavior for the clear ip dhcp conflict command:

- If the **pool** *NAME* option is not specified and an IP *ADDRESS* is specified, the system parses all the DHCP pools for the address of the specified conflict.
- If the **pool** *NAME* option is not specified and no IP *ADDRESS* is specified, then the system deletes all address conflicts from all DHCP pools.
- If the **pool** *NAME* option is specified but no IP *ADDRESS* is specified, then all conflicts in the specified pool will only be cleared.
- If both the **pool** *NAME* option and an IP *ADDRESS* are specified, the specified address conflict will be deleted from the specified pool.

Examples The following example shows an address conflict of 10.12.1.99 being deleted from the DHCP server database

```
switch# clear ip dhcp conflict 10.12.1.99
switch#
```

The following example deletes all the address conflicts from the entire DHCP server database.

```
switch#clear ip dhcp conflict
switch#
```

The following example deletes all the address conflicts from the address pool named pool1:

```
switch#clear ip dhcp conflict pool pool1
switch#
```

clear ip dhcp server statistics

Use this command to reset all Dynamic Host Configuration Protocol (DHCP) server counters.

clear ip dhcp server statistics

Syntax None

Default None

Command Mode Privileged EXEC

Usage Guideline This command clears all of the DHCP statistic counters. That is all of counters will be initialized, or set to zero.

Example The following example resets all DHCP counters to zero.

```
switch# clear ip dhcp server statistics
switch#
```

clear ip ospf

Use this command to restart the OSPF process.

clear ip ospf

Syntax None

Default None

Command Mode Privileged EXEC

Usage Guideline This command is used to restart the OSPF routing process. The following is a situation where this command can be used:

- When a new route-ID is configured, it will not take effect until next time the switc h is booted. When the OSPF process is restarted by this command, the new router-ID will take effect immediately without having to reboot the switch.

Example This example shows how to restart all of OSPF processes

```
Switch>enable
Switch# clear ip ospf
```

clear ipv6 dhcp client

This command is used to restart the DHCPv6 client on an interface.

clear ipv6 dhcp client *INTERFACE-NAM***E**

Syntax Description	
INTERFACE-NAME	Specifies the identifier of the switch interface on which to restart the DHCPv6 client.

Default None

Command Mode Privileged EXEC

Usage Guideline The **clear ipv6 dhcp client** command restarts DHCP for an IPv6 client on a specified interface after first releasing and unconfiguring the previously acquired prefixes and other configuration options (for example, Domain Name System [DNS] servers).

Example The following example restarts the DHCPv6 client for interface vlan1:

```
Switch > enable
Switch # clear ipv6 dhcp client vlan1
Success.
Switch #
```

clear ipv6 neighbors

This command is used to clear the IPv6 neighbor information.

clear ipv6 neighbors [IFNAME]

Syntax None

Default None

Command Mode Privileged EXEC

Usage Guideline The command **clear ipv6 neighbors** will only clear dynamic entries.

Example This example shows how to clear instances of IPv6 neighbors:

```
Switch > enable
Switch # clear ipv6 neighbors vlan1
Switch #
```

clear ipv6 ospf process

To restart the state of IPv6 OSPF, use the **clear ipv6 ospf process** command.

clear ipv6 ospf [*PROCESS-ID***] process**

Syntax Description	
PROCESS-ID	(Optional) Internally used identification parameter for an IPv6 OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each IPv6 OSPF routing process.

Default None

Command Mode User EXEC

Usage Guideline When the **clear ipv6 ospf process** command is used, the IPv6 OSPF database is cleared and repopulated. Once the database is cleared and repopulated the SPF algorithm will be performed.

Use the *PROCESS-ID* option to clear only one IPv6 OSPF process. If the *PROCESS-ID* option is not specified, all IPv6 OSPF processes are cleared.

Example The following example restarts the SPF algorithm by clearing the IPv6 OSPF processes from the database.

```
Switch > enable
Switch # clear ipv6 ospf process
```

clear ipv6 rip

To delete routes from the IPv6 RIP routing table, use the **clear ipv6 rip** command.

clear ipv6 rip

Syntax None

Default None

Command Mode Privileged EXEC

Usage Guideline All IPv6 RIP routes are deleted.

Examples The following example deletes all the IPv6 routes for the RIP process.

```
Switch > enable
Switch # clear ipv6 rip
```

clear lldp neighbors

Use this command to delete all LLDP information learned from neighboring devices.

clear lldp neighbors [interface *INTERFACE-ID* **[, | -]]**

Syntax

INTERFACE-ID	(Optional) Delete LLDP neighboring information for a specific interface. Valid interfaces are physical interface
,	(Optional) Specifies a series of physical interfaces. No space before and after the comma.
-	(Optional) Specifies a range of physical interfaces. No space before and after the hyphen.

Default None

Command Mode Privileged EXEC mode

Usage Guideline If the command clear lldp neighbors is issued without interface keyword, all neighboring information on all interfaces will be deleted.

Example This example shows how to delete all neighboring information on all interfaces:

```
Switch# clear lldp neighbors
```

clear lldp statistics

Use this command to delete LLDP statistics.

clear lldp statistics [interface *INTERFACE-ID* [, | -]]

Syntax

interface *INTERFACE-ID*	(Optional) Specifies the interface to clear LLDP neighboring information. Valid interfaces are physical interface
,	(Optional) Specifies a series of physical interfaces. No space before and after the comma.
-	(Optional) Specifies a range of physical interfaces. No space before and after the hyphen.

Default Not applicable

Command Mode Privileged EXEC mode

Usage Guideline You can use this command with interface keyword to reset LLDP statistics of the specified interface(s). If the command clear lldp statistics is issued without interface keyword, only global LLDP statistics will be cleared.

Example This example shows how to reset all LLDP statistics:

```
Switch# clear lldp statistics
```

.

clear logging

Use this command to clear log messages from the system logging buffer.

clear logging

Syntax None

Default None

Command Mode Privileged EXEC

Usage Guideline Use this command to clear log messages from the logging buffer.

Example The following example to show how to clear log messages in buffer.

```
Switch> enable
Switch# clear logging
Switch#
```

clear mac address-table

Use the **clear mac address-table** command to delete from the MAC address table:

- specific dynamic address,
- all dynamic addresses on a particular interface,
- all dynamic addresses,
- or all dynamic addresses on a particular VLAN.

clear mac address-table { dynamic [address *MAC-ADDR* **| interface** *INTERFACE-ID* **| vlan** *VLAN-ID* **] }**

Syntax Description	
address *MAC-ADDR*	Delete the specified dynamic MAC address.
interface *INTERFACE-ID*	The specified interface can be a physical port or port-channel.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

Default None

Command Mode Privileged EXEC

Usage Guideline When using the **address** *MAC-ADDR* argument, only the dynamic entries will be cleared.

Example This example shows how to remove a specific MAC address from the dynamic address table:

```
Switch# clear mac address-table dynamic address 00:08:00:70:00:07
```

Verify the information was deleted by entering the **show mac address-table** command.

clear port-security

To delete all of the secured MAC addresses, except for manually configured secured MAC addresses, from the MAC address table, use the **clear port-security** command.

clear port-security [{address *MAC-ADDR* **} | {interface** *INTEFACE-ID* **}] [vlan** *VLAN-ID***]**

Syntax Description	
address *MAC-ADDR*	(Optional) Deletes the specified secure MAC address auto-learned.
Interface *INTEFACE-ID*	(Optional) Deletes all secure MAC addresses auto-learned on the specified physical.
vlan *VLAN-ID*	(Optional) Deletes the specified secure MAC address from the specified VLAN.

Default None

Command Mode Privileged EXEC

Usage Guideline This command clears secure MAC address that are auto-learned only and not manually configured MAC addresses.

If the **clear port-security** command is entered without adding any keywords or arguments, the switch removes all the secure MAC addresses from the MAC address table.

If the **clear port-security interface** *INTERFACE-ID* command is entered, all the secure MAC addresses auto-learned on the specified interface are removed from the MAC address table.

Example This example shows how to remove a specific secure address from the MAC address table:

```
Switch# clear port-security address 0080.0070.0007
Switch#
```

This example shows how to remove all the secure MAC addresses auto-learned on a specific interface:

```
Switch# clear port-security interface eth3.1
```

clear running-config factory-defaults

Use this command to clear the system's running configuration.

clear running-config factory-defaults

Syntax None

Command Mode Privileged EXEC at level 15

Usage Guideline The user can enter the **clear running-config factory-defaults** command to clear the system configuration retained in Dynamic RAM.

Before using the **clear running-config factory-defaults** command, save a backup of the configuration using the **copy** command or upload a configuration profile into the system. When the **clear running-config factory-defaults** command is entered, the system resets the running configuration with the factory default settings.

Since the command clears all of system configuration settings including IP parameters, any remote management applications will loose their connections. Therefore, before proceeding, a confirmation should be applied. In addition, it is suggested to reload a configuration file immediately after clearing the configuration.

The **clear running-config** command clears all system configuration settings including the MGMT-IP address which is set back to the factory default of 10.90.90.90/8.

Example The following example demonstrates how to clear system running configuration.

```
Switch# clear running-config factory-defaults
.............................
Switch#
```

clear spanning-tree detected-protocols

To restart the protocol migration, use the **clear spanning-tree detected-protocol** command.

clear spanning-tree detected-protocols [interface *INTERFACE-ID* **]**

Syntax Description	
interface *INTERFACE-ID*	(Optional) Specifies the port interface that will trigger the detecting action. If no option is specified, every port is effected by this command.

Default None

Command Mode Privileged EXEC.

Usage Guideline This configuration is only effective for RSTP version or MSTP mode. By issuing the command the port protocol migrating state machine will be forced to SEND_RSTP state. This action can be used to test whether all legacy bridges on a given LAN have been removed. If there is no STP Bridge on the LAN, the port will operate in the configured mode, either in RSTP or MSTP mode. Otherwise, the port will operate in STP mode.

RSTP and MST have built-in compatibility mechanisms that allow them to interact properly with other versions of IEEE spanning tree or other regions. For example, a bridge running RSTP can send 802.1D BPDUs on one of its ports when it is connected to a legacy bridge. An MST bridge can detect that a port is at the boundary of a region when it receives a legacy BPDU or an MST BPDU that is associated with a different region. These mechanisms are not always able to revert to the most efficient mode. For example, an RSTP bridge that is designated for a legacy 802.1D stays in 802.1D mode even after the legacy bridge has been removed from the link. Similarly, an MST port assumes that it is a boundary port when the bridges which it is connected to have joined the same region. To force the MST port to renegotiate with the neighbors, enter the cl**ear spanning-tree detected-protocol** command.

Entering the **clear spanning-tree detected-protocol** command with no arguments, applies the command to every port of the switch.

Example This example shows how to trigger the protocol migration event for all ports:

```
Switch# clear spanning-tree detected-protocols
```

clear vlan-tunnel ctag-mapping dynamic

Use this command to clear all dynamically learned mappings between customer VLAN tags and source IPs.

clear vlan-tunnel ctag-mapping dynamic

Syntax None

Default None

Command Mode User EXEC

Usage Guideline This command is used to clear all dynamically learned mappings between a customer VLAN tag and source IP in the switch software. When the setting of a VLAN tunnel is changed, as for example its interface-type or TPID, then the new setting could for example cause the system to send out control packets with the wrong customer VLAN tag. In this situation, use this command to clear the incorrect dynamically learned mapping entries to re-learn the correct customer VLAN tag mapping with the source IP.

Examples This example shows how to clear all dynamically learned customer VLAN tag mappings.

```
Switch# clear vlan-tunnel ctag-mapping dynamic
Switch#
```

clock set

Use this command to manually set the system clock.

clock set *HH:MM:SS DAY MONTH YEAR*

Syntax Description	
HH:MM:SS	Current time in hours (24-hour format), minutes and seconds.
DAY	Current day (by date) in the month.
MONTH	Current month (by name, January, Jan, February, Feb, and so on).
YEAR	Current year (no abbreviation).

Default Hardware Generated - 00:00:00 01 January 1993

Command Mode Privileged EXEC at Privilege level 15

Usage Guideline Generally, if the system is synchronized by a valid outside timing mechanism, such as SNTP, it is not necessary to set the clock manually. Use this command if no other time sources are available. Use the **clock timezone command on page 119** to configure the timezone applied to the clock settings. The clock configured by this command will be applied to RTC if it is available. The configured clock will not be stored in the configuration file.

If the clock is manually set and the SNTP server is configured, the system will still try to sync the clock with the server. If time sync is successful, the SNTP server set time replaces the manually set time.

If the SNTP state changes from enabled to disabled, the system clock continues operations but no longer attempts to sync time with the server.

Example The following example shows how to manually set the software clock to 6:00 p.m. on Aug 22, 2010:

```
Switch# clock set 18:00:00 22 Aug 2010
Switch#
```

Verify the settings by entering the **show clock** command.

clock summer-time

Use one of the optional keyword formats of the **clock summer-time** command to configure the system time to automatically set the seasonal time adjustment (daylight saving time). To disable automatic seasonal time adjustment, use the no form of this command.

clock summer-time recurring *WEEK DAY MONTH HH:MM WEEK DAY MONTH HH:MM* **[** *OFFSET* **]**

clock summer-time date *DATE MONTH HH:MM DATE MONTH HH:MM* **[** *OFFSET* **]**

no clock summer-time

Syntax Description	
recurring	Indicates that a summer seasonal time change should start and end on the specified day and week of the specified month. For example: summer time adjustment begins Sunday in the first week of April.
date	Indicates that summer time should start and end on the specified date of the specified month.
WEEK	Week of the month (1 to 4 or last).
DAY	Day of the week (sun, mon, and so on).
DATE	Date of the month (1 to 31).
MONTH	Month (by name , January, February, and so on).
HH:MM	Time (24 hours format) in hours and minutes.
OFFSET	(Optional) Number of minutes to add during summer time (default is 60)The range of offset is 30, 60, 90 and 120.

Default Disabled

OFFSET: 60

Command Mode Global configuration

Usage Guideline Use this command to automatically make seasonal time changes for the system clock.

The **recurring** mode is used to make time adjustment to begin and end on a specified week day, week and month. Use the **date** mode to make the time change begin and end on specified calender dates. The syntax for both modes uses the first portion of the parameter to express the begining of the time adjustment period while the ending of the period is expressed in the second portion.

Example The following example shows how to specify that summer time starts on the first Sunday in April at 2 a.m. and ends on the last Sunday in October at 2 a.m:

```
Switch# configure terminal
Switch(config)# clock summer-time recurring 1 sun April 2:00 last sun October 2:00
Switch(config)# end
```

Verify the settings by entering the **show clock** command.

clock timezone

Use the command to set the time zone for display purpose. To set the time to Coordinated Universal Time (UTC), use the no form of this command.

clock timezone {+|-} *HOURS-OFFSET* **[** *MINUTES-OFFSET* **]**

no clock timezone

Syntax Description	
+|-	'+' means time to be added to the UTC; '-' means time to be subtracted from the UTC.
HOURS-OFFSET	Hours difference from UTC.
MINUTES-OFFSET	(Optional) Minutes difference from UTC.

Default UTC

Command Mode Global configuration

Usage Guideline The time obtained by SNTP server refers to the UTC time. The local time will be calculated based on UTC time, time zone, and the daylight saving configuration.

Example The following example shows how to set the time zone to Pacific Standard Time (PST), which is 8 hours behind UTC:

```
Switch# configure terminal
Switch(config)# clock timezone - 8
Switch(config)# end
```

Verify the settings by entering the **show clock** command.

color-aware

Use the **color-aware** command to specify the color aware mode for a class. Use the no form of the command to set the class to color blind mode.

color-aware

no color-aware

Syntax None

Default color-blind mode

Command Mode Policy-map class configuration

Usage Guideline The **color-aware** command specifies that the configured policer for the traffic class will operate in color aware mode. In color aware mode, the initial color of the packet and the policer metering result determines the final color. The initial color of the packet is mapped from the incoming DSCP based on the DSCP to color map if the receiving port trusts DSCP. If the receiving port trusts CoS, then the initial color is mapped from the incoming CoS based on the CoS to color map

If the configured policer operates in color blind mode, then the policer metering result determines the final color.

Examples The following example creates the policy map pcolor-map1 and configures the policy of running color aware mode and two rate policing for the class1 class in the policy map.

```
Switch(config)# policy-map pcolor-map1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# color-aware
Switch(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000
exceed-action set-dscp-transmit 2 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

The following example attach the pcolor-map1 policy map to eth3.1 and sets the port to trust CoS and defines the CoS to color map.

```
Switch(config)# interface eth3.1
Swtich (config-if)# service-policy pcolor-map1
Swtich (config-if)# qos trust cos
Swtich (config-if)# qos map cos-color 1-7 to green
Swtich (config-if)# exit
```

Verify the settings by entering the **show policy-map** command.

command prompt

Use this command to change the device cli prompt to, for example: the product name, system name, or other user-defined strings. The command can also specify whether to display the current privilege level in the prompt.

command prompt [level | no-level] [string *STRING* **| product-name | system-name]**

Syntax Description	
level	(Optional) The privilege level information is appended to prompt name.
no-level	(Optional) No privilege level information is appended to prompt name.
string *STRING*	(Optional) Specifies the user-defined prompt. The valid length is 1-8 characters. The syntax is a user-defined string.
product-name	(Optional) Use the product name as the prompt name
system-name	(Optional) Use the system name (as defined in SNMP System group MIB) as the prompt name.

Default **product-name** with privilege **level**

Command Mode Privileged EXEC

Usage Guideline The prompt refers to the string that appears indicatng to a user to input a command. It consists of two parts. The first part is the prompt name. The second part is the privileged level.

Using this command, the user can change the prompt to use either the product name or system name and specify whether or not to display the privilege level in the prompt

Either one or both settings can be changed. If the user selects to use the product name or the system name as the prompt, only the first 8 characters are taken.

The prompt will be changed immediately after the command is executed.

Examples This example shows how to change the prompt to use the system name.

```
DGS-6600:15# command prompt system-name
switch:15#
```

The following example shows how to set the command prompt back to default setting: (product name and privilege level).

```
switch:15# command prompt
DGS-6600:15#
```

The following example shows how to hide the privilege information from the console prompt.

```
DGS-6600:15# command prompt no-level
DGS-6600#
```

This example shows define alpha as the console prompt.

```
DGS-6600:15# command prompt level string alpha
alpha:15#
```

configure terminal

Use this command to enter the global configuration mode

configure terminal

Syntax None

Default None

Command Mode Privileged EXEC

Usage Guideline Entering into the configuration mode allows configuration settings of the switch to be entered or modified i.e. performing switch configuration.

Example This example shows how to enter into the configuration mode:

```
Switch#configure terminal
Switch(config)#
```

copy

Use the **copy** command to copy a image, log or configuration file from a remote or local source to a local or remote destination file.

copy *SOURCE-URL DESTINATION-URL*

copy *SOURCE-URL* **tftp:** *{IP-ADDRESS | IPv6-ADDRESS}* **\[** *DIRECTORY* **\]** *FILENAME*

copy tftp: *{IP-ADDRESS | IPv6-ADDRESS}* **\ [** *DIRECTORY* **\ ]** *FILENAME DESTINATION-URL*

Syntax Description

SOURCE-URL	Specifies the source URL for the source file to be copied. The URL has two forms. One of them is represented by keyword. For the second form, it is prefixed by the media. The acceptable media are flash:\ and cf1:\. Flash:\ refers to system internal on-board FLASH memory cf1:\ represents the first opened slot compact FLASH memory. The source can be either local or remote. For download purpose, the source is in remote server. For upload purpose, the source is located locally. If the *running-config* is specified as the *SOURCE-URL*, the purpose is to upload the running configuration or save the running-configuration as the startup configuration. If the system-log is specified as the *SOURCE-URL*, the system log can be retrieved to TFTP server. If the *startup-config* is specified as the *SOURCE-URL*, the purpose is to upload the startup configuration and save it as: a file in the file system or as the running-configuration.
DESTINATION-URL	Specifies the destination URL as the target for the copied file. The URL has two forms. One of them is represented by keyword. For the second form, it is prefixed by media. The acceptable media are flash:\, cf1:\. Flash:\ refers to system internal on-board FLASH memory cf1:\ represents the first opened slot compact FLASH memory. The destination can be either local or remote. When downloading the destination is target is the local file system. When uploading the destination is on a remote server. When *running-config* is specified as the *DESTINATION-URL,* it will write the source file contents as the running configuration. When *startup-config* is specified as *DESTINATION-URL*, the source file contents will be saved as the next-boot configuration. It will saved into the current configuration file in NVRAM and the file name will be maintained as the file name specified with **boot config** command.

IP-ADDRESS\	The IP address of TFTP server.
DIRECTORY\	The directory name of the source or destination file in TFTP server.

Default None

Command Mode Privileged EXEC

Level 15 for configuration copy.

Usage Guideline The **copy** command (when the source/destination URL is running-config, startupconfig is only available at privilege level 15.

Use this command to download or upload the image file or the configuration file between remote TFTP server and the local file system. Also use this command to upload system log to TFTP server.

The **copy** *SOURCE-URL DESTINATION-URL* command is used to copy file from system flash to compact flash or vice versa.

To upload the running configuration or save the running-configuration to startup configuration, specify *running-config* as the *SOURCE-URL*. To save it to the startup config, specifies *startup-config* as the *DESTINATION-URL*.

Notice: If the destination is the *startup-config* file, the source file is directly copied to the file specified in **boot config** command. This means the original *startup-config* file is overwritten by the running configuration.

To apply a configuration file to the running configuration, specify *running-config* as the *DESTINATION-URL*.

Notice: If the source is a system-log and the destination is a file, the current system log information is saved to NVRAM with the specified name. Be aware that any **copy** *running-config* action does not imply any system log copy or saving action.

To represent a file in the remote TFTP server, the URL must be prefixed with tftp:.

If the *SOURCE-URL* or *DESTINATION-URL* is a tftp server, it uses switch port to connect the network under execution mode. Under management mode It uses the management port to connect the network. .

In this chassis based switch, the runtime image also contains the operational code for the line cards. The operational code is automatically synced to the line card during the boot-up procedure.

Any file to be downloaded (or copied) to the directory to be an image file in the system's flash or downloaded (or copied) to be the startup-image will be checked and verified whether it is an image file with a correct checksum and model ID.

Any file to be downloaded (or copied) as the startup-config or the running-config will be checked and verified whether it is a configuraiton file or not (the **boot config** command will also check whether it is a configuraiton file or not first).

Examples

This example shows how to configure the switch (running configuration) to use a configuration (switch-config.txt) that is download from a TFTP server(10.1.1.254).

```
Switch# copy tftp:\\10.1.1.254\config\switch-config.txt running-config
Configure using 10.1.1.254\config\switch-config.txt (y/n) [n]? y
Finished network download. (134 bytes)
Apply to system configuration…. Completed.
Switch#
```

This example shows how to upload (retrieve) the running configuration to a TFTP server for storage:

```
Switch# copy running-config tftp:\\10.1.1.254\config\switch-config.txt
Upload configuration to tftp:10.1.1.254 \config\switch-config.txt, (y/
n)[n]? y
Configuration has been copied successfully.
Switch#
```

This example shows how to save the system running configuration into FLASH memory and use it for the next boot configuration:

```
Switch# copy running-config startup-config
Save system configuration (y/n) [n], y
Configuration has been copied successfully.
Switch#
```

cos remarking

Use this command to remark the receiving CoS priority for a VLAN tunnel application. Use the no form of this command to set as customer CoS trusted.

cos remarking *NEW-COS* **[***C-VID* **[, | -]]**

no cos remarking [*C-VID***[, | -]]**

Syntax Description	
NEW-COS	Specifies the new COS value to be added into the outer priority tag for VLAN encapsulation. Alternatively it is used to replace the priority tag for VLAN remarking. The available value is 0~7.
C-VID **[,	-]**	(Optional) Specifies the receiving packet with the inner VLAN (customer VLAN ID, CVID) in this list it will use the new COS value and it will be added into the outer priority tag (in VLAN encapsulation) or is used to replace the priority tag (in VLAN remarking). If *C-VID***[,|]** is not specified for the **no cos remarking** command, then the ingress port will trust the user's priority tag and replicate/retain the priority tag except those customers' VLANs that have been set by **cos remarking NEW-COS C-VID [,	-]** command. If *C-VID***[,|]** is not specified for the **cos remarking NEW-COS** command, then the ingress port will remark the user's priority tag and remark/replace the priority tag except those customers' VLANs that have been set by **cos remarking** *NEW-COS C-VID* **[,	-]** (**cos remarking** *NEW-COS* command is not set at the interface). The available values are 1~4094 and only the *C-VID* has been defined in VLAN encapsulation or VLAN remarking pair that can be accepted by this command. That is, the VLAN encapsulation or VLAN remarking pair must be defined, before the CoS remarking policy is changed.

Default No COS remarking is set. The user/inner cost is trusted at the interface.

Command Mode Interface configuration

Usage Guideline This command is used for UNI port for VLAN tunnel application.

Use the **cos remarking** command to remark the outer tag priority. As CoS remarking is applied for VLAN encapsulation, the new CoS value is added into the outer priority tag. As CoS remarking is applied to VLAN remarking, the new CoS value is used to remark(replace) the priority tag.

To retain the priority from the receiving packet, use **no cos remarking** to make the system replicate or retain the original priority tag value to/as the out-going priority tag. This is also referred as user/inner COS trusted. The COS tag replication is only applied to outer priority tag in VLAN encapsulation and the COS remarking (replacement) is applied for the VLAN remarking.

Use the **no cos remarking** *C-VID* command (with optional parameters) to set the related *C-VID* as customer CoS trusted at the interface (**cos remarking** *NEW-COS* command is not set at the interface).

Example

Please follow the below example for a detailed step by step explanation

1. Go to interface Ethernet 4.1

```
Siwthc(config)#>interface eth4.1
```

2. Configure a VLAN encapsulation for C-VID 101-104 to S-VID 1001 and customer CoS trusted.

```
Switch(config-if)#>vlan encapsulation 1001 101-104
```

3. Configure COS remarking for all incoming packets at Ethernet 4.1 as priority of 7.

```
Switch(config-if)#>cos remarking 7
```

4. Remark C-VID 101 packet priority as 3, and others use priority 7 remarking.

```
Switch(config-if)#>cos remarking 3 101
```

5. Change the interface as CoS trusted. That is C-VID 101 will be priority remarking, C-VID 102-104 still remained in customer CoS trusted state, and interface has been set as Customer CoS trusted.

```
Switch(config-if)#>no cos remarking
```

6. The system will trust all of incoming packets CoS, because C-VID is set as Customer CoS trusted now.

```
Switch(config-if)#>no cos remarking 101
```

Verify the settings by entering **show vlan-tunnel** command.

cpu-protect safeguard

Use this command to enable and configure the threshold for Safeguard Engine. Use the **no** form of this command to disable Safeguard Engine.

cpu-protect safeguard [threshold *RISING-THRESHOLD FALLING-THRESHOLD* **]**

no cpu-protect safeguard

Syntax Description	
threshold	Configure the utilization for the Safeguard Engine.
RISING-THRESHOLD	Set a percentage value of the rising CPU utilization which will trigger the Safeguard Engine function. Once the CPU utilization rises over the specified percentage, the Safeguard Engine mechanism will initiate. The valid range is 20 to 100.
FALLING-THRESHOLD	The user can set a percentage value of the falling CPU utilization which will trigger the Safeguard Engine function to cease. Once the CPU utilization falls to the specified percentage, the Safeguard Engine mechanism will shut down. The valid range is 20 to 100.

Default

By default Safeguard_Engine is disabled.

By default rising threshold of CPU utilization is 50.

By default falling threshold of CPU utilization is 20.

Command Mode

Global configuration

Usage Guideline

The Safeguard Engine can help the overall operability of the device by minimizing the workload of the switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth. When the CPU utilization of the switch rises over configured rising threshold, it will enter exhausted mode. In exhausted mode, the switch limits the bandwidth of receiving ARP request and drop all broadcast IP packets. Regarding the way to limit the bandwidth is project dependent.

You can use the command **cpu-protect safeguard** to configure the threshold and enable the Safeguard Engine. The command **no cpu-protect safeguard** is used to disable Safeguard Engine. The command **no cpu-protect safeguard** will reset both the rising and falling thresholds and disable the state of Safeguard Engine.

Example

The following example shows how to configure the thresholds and enable Safeguard Engine. The rising and falling threshold are 60 and 40 respectively.

```
Switch(config)# cpu-protect safeguard threshold 60 40
```

The following example shows how to disable Safeguard Engine and reset threshold to default value.

```
Switch(config)# no cpu-protect safeguard
```

You can verify your settings by entering **show cpu-protect safeguard** command.

cpu-protect type

Use this command to configure the rate-limit of traffic destined to CPU by protocol type.

cpu-protect type *PROTOCOL-NAME* **pps** *RATE*

no cpu-protect type *PROTOCOL-NAME*

Syntax Description	
PROTOCOL-NAME	Specifies the protocol name (for example, **bgp**) to be configured. See the “Usage Guideline” for a list of protocols supported by most routers.
RATE	Specify the threshold. The unit is packets per second. The valid range is project dependent. When set to 0, all packets of the specified protocol are dropped. The max *RATE* is 2000.

Default None

Command Mode Global configuration

Usage Guideline CPU must handle certain packets, such as routing protocols, Layer 2 protocols, and packets for management. If the traffic destined to CPU overloads, the CPU will spend much time processing unnecessary traffic, and the routing processes are impacted. To mitigate the impact, the user can use this command to control the threshold of individual protocol packets. When the **no**-form of this command is configured, the related counter will reset to zero.

Supported Protocols that can be configured rate-limit:

The following table lists the reference for the supported protocols for the cpu-protect type command. According to the purpose of packets destined to CPU, the router creates three virtual sub-interfaces to process the packets:

- **manage:** The packets are destined to one of the router interfaces via the interactive access protocol, such as Telnet and SSH.
- **protocol:** The packets are protocol control packets which can be identified by the router.
- **route:** Others, packets traversing the router for routing that must be processed by the router CPU (e.g. software routing) before it can be routed without CPU's involvement.

The classification of each protocol lists at the column of "Classification (sub-interface)".

Table 1 Supported protocol name for the command **cpu-protect type**

Protocol Name	Description	Classification (sub-interface)
arp	IP Address Resolution Protocol (ARP)	protocol
bgp	Border Gateway Protocol (IPv4)	protocol
dhcp	Dynamic Host Configuration (IPv4)	protocol
dhcpv6	Dynamic Host Configuration (IPv6)	protocol
dot1x	Port Based Network Access Control	protocol
dvmrp	Distance Vector Multicast Routing Protocol (IPv4)	protocol
gvrp	GARP VLAN Registration Protocol	protocol
icmp	Internet Control Message Protocol (IPv4)	protocol
icmpv6-ndp	ICMP Neighbor Discover Protocol (NS/NA/RS/RA/Redirect, IPv6)	protocol
icmpv6-other	ICMP except NDP NS/NA/RS/RA/Redirect (IPv6)	protocol
igmp	Internet Group Management Protocol(IPv4)	protocol
lacp	Link Aggregation Control Protocol	protocol
ospf	Open Shortest Path First (IPv4)	protocol
ospfv3	Open Shortest Path First (IPv6)	protocol
pim	Protocol Independent Multicast (IPv4)	protocol
rip	Routing Information Protocol (IPv4)	protocol
ripng	Routing Information Protocol (IPv6)	protocol
snmp	Simple Network Management Protocol (IPv4/IPv6)	manage
ssh	Secured shell (IPv4/IPv6)	manage
stp	Spanning Tree Protocol (802.1D)	protocol
telnet	Telnet (IPv4/IPv6)	manage
vrrp	Virtual Router Redundancy Protocol (IPv4)	protocol
web	HTTP (IPv4)	manage

Example The following example shows how to set threshold of OSPF protocol packet as 100 packets per second.

```
Switch(config)# cpu-protect type ospf pps 100
```

The following example shows how to remove threshold of OSPF protocol packet.

```
Switch(config)# no cpu-protect type ospf
```

Verifying the settings by **show cpu-protect** type command.

cpu-protect sub-interface

Use this command to configure the rate-limit for traffic destined to CPU by sub-interface type.

cpu-protect sub-interface { manage | protocol | route } pps *RATE*

no cpu-protect sub-interface { manage | protocol | route }

Syntax Description	
RATE	Specify the threshold. the unit is packets per second. The valid range is project dependent. When set to 0, all packets of the specified sub-interface type will be dropped. The max *RATE* is 2000

Default none

Command Mode Global Configuration

Usage Guideline The reasons of packets are destined to CPU can be classified into three groups: **manage**, **protocol** and **route**. The sub-interface is a logical interface, which handles the CPU received packets by different groups. Generally speaking, the protocol packets should have higher priority to make sure the functions work normally. CPU usually does not involve in the routing packets. In few cases, such as leaning new IP address or default route is not specified, some packets will be sent to CPU for software routing. The user can use this command to limit the rate of routed packets to avoid CPU spending too much time for routing packets. The classification of each protocol type lists at Table 1. When the no-form of this command is configured, the related counter will reset to zero.

Example The following example shows how to set rate limit of manage packet group, and set threshold to 1000 packets per seconds.

```
Switch(config)# cpu-protect sub-interface manage pps 1000
Switch#
```

The following example shows how to remove rate-lilmit of management traffic.

```
Switch(config)# no cpu-protect sub-interface manage
Switch#
```

Verifying the settings by **show cpu-protect sub-interface** command.

crypto key

To generate and configure an RSA or DSA key pair, use the **crypto** key command.

crypto key { rsa|dsa } *NBITS* **[force]**

Syntax Description	
rsa	Configure an RSA key pair.
dsa	Configure a DSA key pair.
NBITS	Specifies the size of the key pair(s): For RSA the valid values are 512, 768, 1024, and 2048. For DSA the valid values are 512, 768, and 1024. For SSH version 2, the minimum recommended key size is 768 bits. A key size with a larger number provides higher security but takes longer to generate.
force	(Optional) Regenerates the keys and suppresses the warning prompt for overwriting existing keys.

Default None

Command Mode Privileged EXEC

Usage Guideline To support SSH login, an RSA or DSA key pair must first be generated. This command can generate either an RSA or DSA key to provide greater security when logging into the server using SSH. The NBITS value is required to specify the size of the key pair.

Example This example shows how to create an RSA key, 1024 bits:

```
Switch# crypto key rsa 1024
Generating RSA keys.... [OK]
Switch#
```

default-gateway (management port)

Use this command to set the IP address of the default gateway. Use the no form of this command to revert to the default value.

default-gateway *IP-ADDRESS*

no default-gateway

Syntax Description	
IP-ADDRESS	IP address in four-part dotted decimal format.

Default *IP-ADDRESS*: 0.0.0.0.

Command Mode Management interface

Usage Guideline The management port will send out IP packets for other IP subnets through this IP address.

Example This example shows how to set 10.1.1.254 as the IP address of the default gateway.

```
switch#configure terminal
switch(config)#
switch(config)#mgmt-if
switch(mgmt-if)#default-gateway 10.1.1.254
switch(mgmt-if)#end
```

Verify the settings by entering the **show mgmt-if** command

default-information originate (BGP)

Use this command to configure a Border Gateway Protocol (BGP) routing process to distribute a default route (network 0.0.0.0), use the **default-information originate** command in address family or router configuration mode. To disable the advertisement of a default route, use the **no** form of this command.

default-information originate

no default-information originate

Syntax Description None

Default None

Command Mode Router configuration

Address family configuration

Usage Guideline The default-information originate command is used to configure a BGP routing process to advertise a default route (network 0.0.0.0). A redistribution statement must also be configured to complete this configuration or the default route will not be advertised.

The configuration of the default-information originate command in BGP is similar to the configuration of the network (BGP) command. The default-information originate command, however, requires explicit redistribution of the route 0.0.0.0. The network command requires only that the route 0.0.0.0 is present in the Interior Gateway Protocol (IGP) routing table. For this reason, the network command is preferred.

Example This example shows how to advertise the default route regardless whether a default route exists in the configuration or not.

```
Switch(config)# router bgp 65534
Switch(config-router)# default-information originate
```

Verify the settings by entering the **show ip protocols BGP** command.

default-information originate (IPv6 OSPF)

Use **default-information originate** to configure an IPv6 OSPF to generate a default external route (type 0x4005 LSA). Use the no form of the command to disable the originate type 0x4005 LSA default route.

default-information originate [always] [metric *METRIC-VALUE***] [metric-type** *TYPE-VALUE***]**

no default-information originate

Syntax Description	
always	(Optional) Always advertise the default route regardless whether a default route exists in the configuration or not.
metric *METRIC-VALUE*	(Optional) If **metric** is not specified, the default metric is 1. The range off values allowable for the OSPFv3 metric is from 0-16777214.
metric-type *TYPE-VALUE*	(Optional) IPv6 OSPF specifies the external link type associated with the default route advertised into the IPv6 OSPF routing domain. It can be one of two values: 1: Type 1 external route 2: Type 2 external route If a metric-type is not specified, the Switch adopts a Type 2 external route. This is only for IPv6 OSPF.

Default None

Command Mode Router configuration

Usage Guideline The **default-information originate** command is used to configure a routing process, in order to advertise a default route (prefix ::/0). When **always** is not specified, the default route will only be advertised when the redistribution statement is configured and the default route exists in the redistributed routes.

Example This example shows how to advertise the default route regardless whether a default route exists in the configuration or not.

```
Switch > enable
Switch # configure terminal
Switch (config) # router ipv6 ospf
Switch(config-router)# default-information originate always
```

default-information originate (RIP)

To generate a default route into Routing Information Protocol (RIP), use the **default-information originate** command. To disable this feature, use the no form of this command.

default-information originate

no default-information originate

Syntax None

Default Disabled

Command Mode Router configuration

Usage Guideline Issuing this command generates a default route into RIP. The metric will always be one.

Example The following example shows how to generate a default route into RIP:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# default-information originate
```

Verify the settings by entering the **show running-config** command.

default-information originate (RIP IPv6)

To originate a default IPv6 route into RIP, use the **default-information originate** command. To remove the default IPv6 RIP route, use the no form of this command.

default-information originate

no default-information originate

Syntax None

Default Disabled

Command Mode Router configuration

Usage Guideline Originating a default IPv6 route into RIP also forces the advertisement of the route in router updates sent on the interface. The advertisement of the route occurs regardless of whether the route is present in the IPv6 routing table.

Example The following example originates a default IPv6 route into RIP and advertises the default route with all other routes.

```
Switch > enable
Switch # configure terminal
Switch (config) # router ipv6 rip
Switch (config-router) # default-information originate
```

default ipv6 nd prefix

This command is used to default the IPv6 RA prefix information.

default ipv6 nd prefix *X:X::X:X/M*

Syntax Description	
X:X::X:X/M	IPv6 network address. This argument must be in the form documented in RFC2373 where the address is specified in hexadecimal using 16-bit value between colons. X:X::X:X: IPv6 address M: IPv6 prefix length

Default None

Command Mode VLAN interface configuration

Usage Guideline RA prefix entry must be created first.

Example This example shows how to default the IPv6 nd prefix instance:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # default ipv6 nd prefix 3ffe:501:ffff::/64
Switch (config-if) #
```

default-metric (OSPF)

To set default metric values for OSPF, use the **default-metric** command. Use the no form of the command to remove the default-metric setting.

default-metric *METRIC-VALUE*

no default-metric

Syntax Description	
METRIC-VALUE	Default metric value appropriate for the specified routing protocol.

Default *1*

Command Mode Router configuration

Usage Guideline The **default-metric** command is used in conjunction with the **redistribute** router command (redistribute command on page 502) to cause the current routing protocol to use the same metric value for all redistributed routes.

A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

The setting precedence that determines the metric is:

metric in redistributed command > default-metric setting.

Example The following example shows a router redistributing RIP-derived routes into the OSPF domain and all redistributed routes are advertised with an OSPF metric of 10.

```
Switch(config)# router ospf
Switch(config-router)# default-metric 1
Switch(config-router)# redistribute rip
Switch(config-router)# end
Switch#
```

default-metric (IPv6 OSPF)

To set the default metric for IPv6 OSPF, use the **default-mertic** command. To return the metric to its default value, use the no form of this command.

default-metric *METRIC-VALUE*

no default-metric [*METRIC-VALUE***]**

Syntax Description	
METRIC-VALUE	Default metric value. A number from 1 to 16777214.

Default *METRIC-VALUE*: 20

Command Mode Router configuration

Usage Guideline The default-metric command is used in conjunction with the **redistribute** router configuration command (redistribute (IPv6 OSPF) command on page 505) to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with an incompatible metric. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

The order of the setting precedence to determine the metric is:

set metric in redistributed command > default-metric setting.

Example The following example shows an IPv6 OSPF redistributing routes from RIP. All redistributed routes are advertised with a metric of 10.

```
Switch > enable
Switch # configure terminal
Switch (config) # router ipv6 ospf
Switch (config-router) # default-metric 10
Switch (config-router) # redistribute rip
```

default-metric (RIP)

To set default metric values for Routing Information Protocol (RIP), use the **default-metric** command. To return to the default state, use the default form of the command.

default-metric *METRIC-VALUE*

default default-metric

Syntax Description	
METRIC-VALUE	Default metric value. (From 1 to 16).

Default 1

Command Mode Router configuration

Usage Guideline The default-metric command is used in conjunction with the **redistribute** router configuration (**redistribute (RIP) command on page 507**) command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default-metric provides a reasonable substitute and enables the redistribution to proceed.

Example The following example shows how to configure the default metric 5 to redistribute the OSPF routes. In other words, it assigns the OSPF-derived routes a RIP metric of 5. Note that the command **redistribute ospf** without a metric option, causes the OSPF redistribution to use the default metric.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# default-metric 5
Switch(config-router)# redistribute ospf
```

Verify the settings by entering the **show ip protocols rip** command.

default-metric (RIP IPv6)

To set the default metric for IPv6 RIP, use the default-metric. To return the metric to its default value, use the no form of this command.

default-metric *METRIC-VALUE*

no default-metric [*METRIC-VALUE* **]**

Syntax Description	
METRIC-VALUE	Default metric value. A number from 1 to 16.

Default The default metric value is 1

Command Mode Router configuration

Usage Guideline The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with an incompatible metric. Whenever metrics cannot convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

Example The following example shows IPv6 RIP redistributing routes from OSPF. All redistributed routes are advertised with a metric of 10.

```
Switch > enable
Switch # configure terminal
Switch (config) # router ipv6 rip
Switch (config-router) # default-metric 10
Switch (config-router) # redistribute ospf
```

default-router

This command specifies the default router list for a DHCP client. Use the no form of this command to remove the default router list.

default-router *IP-ADDRESS*

no default-router [*IP-ADDRESS***]**

Syntax Description	
IP-ADDRESS	Specifies the IP address of the default-router to DHCP clients.

Default None

Command Mode DHCP pool configuration

Usage Guideline The IP address of the router should be on the same subnet as the client subnet. If the number of servers is more than one, then execute this command multiple times with different server IP addresses. Routers are listed in order of preference (address1 is the most preferred router, address2 is the next most preferred router, and so on).

Exmaple This example shows how to specify 10.1.1.1 as the IP address of default-router in DHCP address pool.

```
switch# configure terminal
switch(config)# ip dhcp pool pool1
switch(config-dhcp)# default-router 10.1.1.1
```

delete

Use this command to delete a file.

delete *FILE-SYSTEM:* **[** *PATH-NAME* **]** *FILE-NAME*

Syntax Description	
FILE-SYSTEM	Specifies the file system.The valid values are *flash* or *cf1*. *flash* represents the Compact FLASH storage of the control management unit. cf1 represents the first open slot of compact FLASH storage .
PATH-NAME	(Optional) Specifies the name of the directory.
FILE-NAME	The file to be deleted.

Default None

Command Mode Privileged EXEC

Usage Guideline A firmware image or a configuration file that is specified as the boot-up file cannot be deleted.

Example This example shows how to delete the file named test from the Flash card inserted in cf1.

If the file to be deleted is used as boot up image or configuration file, then it cannot be deleted and an error message will be displayed.

```
Switch#delete cf1:\test.txt
Delete cf1:\test.txt, (y/n) [n]?
```

description

Use this command to add a description for an interface. Use the **no description** to clear the interface description.

description *DESCRIPTION*

no description

Syntax Description	
DESCRIPTION	Add a description for an interface (up to 128 characters). The syntax is a general string that allows spaces.

Default None

Command Mode Interface configuration

Usage Guideline None

Example This example shows how to add a description for interface eth 3.10

```
Switch(config)# interface eth3.10
Switch(config-if)# description Physical Port 10
```

Verify the settings by entering the **show interface** command.

dir

Use the **dir** command to display the information for a file or the list of files in the specified path name.

dir *FILESYSTEM:* **[** \ *PATH-NAME* **]**

Syntax Description	
FILES-SYSTEM	Specifies the file system. The valid values are flash and cf1; where **flash** represents the compact FLASH (CF) storage of the control management unit and **cf1** represents the compact FLASH storage card inserted in the left slot from the front of the CM module.
PATH-NAME	(Optional) Specifies the name of the directory.

Default None

Command Mode Any EXEC or configuration mode

Usage Guideline None

Example This example displays the list of files on the root directory of the file system on the system's **cf1** flash.

```
Switch>dir cf1:\
log                                                <DIR>
customer                                           <DIR>
system                                             <DIR>
runtime.1.00.017_DGS-6600.had                             64212362 bytes
runtime.1.00.018_DGS-6600.had                              73087296 bytes
Switch>
```

disable

Use this command to return to the User EXEC mode from the Privileged EXEC mode.

disable

Syntax None

Default None

Command Mode Privileged EXEC

Usage Guideline The command will go to the User EXEC level from the power user level.

Example This example shows how to logout after executing the disable command to return to the User EXEC mode.

```
Switch# disable
Switch> logout
```

distance

Use the command **distance** to define an administrative distance for a protocol (RIP, OSPF, etc) or the routes that fall in the range of the specified networks-prefix. Use the no form of the command to remove the distance configuration and then the distance will go back to the default.

distance *DISTANCE [NETWORK-PREFIX/PREFIX-LENGTH]*

no distance *DISTANCE [NETWORK-PREFIX/PREFIX-LENGTH]*

Syntax Description	
DISTANCE	An administrative distance. The default administrative distance for a static route is 1. The range of distance is 1 to 255. The lower value represents a better route.
NETWORK-PREFIX/ PREFIX-LENGTH	(Optional) The network prefix and the prefix length specify the destination network. The Network-Prefix/Prefix-Length parameter is not supported for OSPF.

Default

No static routes are established.

The table below shows the default distance of protocols:

Connected interface	0	The administrative distance of a Connected interface.
Static route	1	The administrative distance of a Static route.
Open Shortest Path First (OSPF)/OSPF6	110	The administrative distance of an OSPF route.
Routing Information Protocol (RIP)/RIPng	120	The administrative distance of a RIP route.
Unknown	255	The administrative distance of an unknown protocol route.

Command Mode

Router configuration

Usage Guideline

This command is only used for routing protocols (RIP, OSPF). The **distance** command of a static route uses the **ip route command on page 309** with the distance option. The distance of local interface can not be configured.

Numerically, an administrative distance is an integer from 1 to 255. In general, the higher the value is, the lower the trust rating is. An administrative distance of 255 means that the routing information source cannot be trusted at all and should be ignored.

Use the **distance** command to set the administrative distance for all the routes that fall in the range of the specified networks-prefix. That is, if the route is in the range of the networks-prefix, the distance specified for the network prefix will be applied to this route.

If the distances for specific routes are not specified, the distances of the routes learned by a routing protocol follows the distance of the routing protocol.

In the current configuration, there is a difference between RIP and RIPng.

1. The specified network prefix means the interface address for RIP.

2. The specified network prefix means the specific routes for RIPng.

If the distances for specific routes are specified, the distances of the routes are set to the specified value.

If the switch is operated at multi-path disabled mode, then the route with the lowest distance will be established as the active route. If the route that is found has failed, then this route will be automatically deactivated and the route with the next lower distance will be the active route.

If the switch is operated in the multi-path enabled mode, then routes with the same distances will be active at the same time.

Note 1: BGP Protocol does not support this command.

Note 2: OSPF does not support the parameter: *[NETWORK-PREFIX/PREFIX-LENGTH]*.

Examples

This example shows how to set rip distance as 100, and route 30.0.0.0/8 with distance 90

```
Switch(config)# router rip
Switch(config-router)# distance 100
Switch(config-router)# distance 90 30.0.0.0/8
```

This example shows how to remove the distance configuration of RIP (set to default distance of RIP, 120) and network 30.0.0.0/8

```
Switch(config)# router rip
Switch(config-router)# no distance 100
Switch(config-router)# no distance 90 30.0.0.0/8
```

Verify the settings by entering the **show ip protocols** command.

dns-server

This command configures the IP address list of DNS servers available to DHCP clients. Use the no form of this command to remove the DNS server list.

dns-server *IP-ADDRESS*

no dns-server [*IP-ADDRESS***]**

Syntax Description	
IP-ADDRESS	Specifies the IP address of DNS server to DHCP clients.

Default None

Command Mode DHCP pool configuration

Usage Guideline This command configures the IP address list of DNS servers available to DHCP clients under the DHCP pool configuration mode. Servers are listed in order of preference. If the number of servers is more than 1, then execute this command multiple times with different server IP addresses.

Example This example shows how to specify 10.1.1.1 as the IP address of DNS server in DHCP address pool.

```
switch# configure terminal
switch(config)# ip dhcp pool pool1
switch(config-dhcp)# dns-server 10.1.1.1
```

domain-name

This command configures the domain name for a DHCP client. Use the no form of this command to remove the domain name.

domain-name *DOMAIN*

no domain-name

Syntax Description	
DOMAIN	Specifies the domain name.

Default None

Command Mode DHCP pool configuration

Usage Guideline This command configures the domain name for a DHCP client.

Example This example shows how to specify domain name as "dlink.com" in a DHCP address pool.

```
switch# configure terminal
switch(config)# ip dhcp pool pool1
switch(config-dhcp)# domain-name dlink.com
```

dos_prevention action

Use this command to specify the action to perform when a DoS attack occurs

dos_prevention action {trap_log }

no dos_prevention action {trap_log}

Syntax Description	
action [*ACTION***]**	Specify the action the device should take when an attacking event occurs. User can specify multiple actions. The **no** form of this command can remove specific actions or all actions. By default drop is enabled and cannot be disabled or enabled by user. **trap_log** The device can be configured to add log or send trap when an attack even happens. When an attacking event occurs continuously, the log or trap will be triggered once every 5 minutes.

Default None

Command Mode Global configuration

Usage Guideline Used to configure actions the device should take when attacking packets received.

Examples The following example shows how to configure for enable action trap_log.

```
Switch# dos_prevention action trap_log
```

The following example shows how to remove action trap_log.

```
Switch# no dos_prevention action trap_log
```

dos_prevention type

Use this command to enable/disable DoS prevention mechanism. The packet matching and actions are handled by hardware. For each type of attack, the device will match the specific pattern automatically.

dos_prevention type {*ATTACK-TYPES* **}**

no dos_preventioin type {*ATTACK-TYPES* **}**

Syntax Description

type *ATTACK-TYPES* Enables the DoS prevention mechanism for etiher a specified or all attacking type. When using the no-form of this command, the specified or all types are disabled.

land_attack

A LAND attack involves IP packets where the source and destination address are set to the address of the target device. It may cause a target device to reply to itself continuously.

blat_attack

This type of attack will send packets with TCP/UDP source ports equal to destination ports of the target device. It may cause a target device to respond to itself.

Caution: use of the blat_attack type option results in suppression of RIP advertisements being transmitted.

smurf_attack

An Attacker sends a large amount of ICMP request packets to an IP broadcast address, the SIP of the attacking packets equals the victim's IP address. If a router delivers traffic to the IP broadcast address, then all host in that IP network will reply with ICMP packets to the victim’s IP address.

tcp_null_scan

Port scanning by using specific packets.

tcp_xmasscan

Port scanning by using specific packets.

tcp_synfin

Port scanning by using specific packets.

tcp_syn_srcport_less_1024

Port scanning by using specific packets.

Syntax Description	- continued
	all All of the above types.

Default Disabled.

DoS prevention of all supported ATTACK-TYPE is disabled.

Command Mode Global configuration

Usage Guideline This command is used to enable/disable the DoS prevention mechanism for specific attack types or for all supported types.

Examples The following example shows how to enable the DoS prevention mechanism for a land_attack.

```
Switch# configure terminal
Switch(config)# dos_prevention type land_attack
```

The following example shows how to enable the DoS prevention mechanism for all supported types.

```
Switch# configure terminal
Switch(config)# dos_prevention type all
```

The following example shows how to disable the DoS prevention mechanism for all supported types.

```
Switch# configure terminal
Switch(config)# no dos_prevention type all
```

dot1v binding protocol-group

Use the **dot1v binding protocol-group** interface configuration command to set a protocol VLAN group and bind VLAN of the port. The no form of this command can remove the port from the specific protocol VLAN group.

dot1v binding protocol-group *GROUP-ID* **vlan** *VLAN-ID*

no dot1v binding protocol-group [*GROUP-ID* **]**

Syntax Description	
GROUP-ID	Specifies the protocol group ID to bind or remove. The valid *GROUP-ID* range is 1 to 16.
VLAN-ID	Specifies the VLAN identifier of the protocol VLAN. Single VLAN ID is valid.

Default The default port is not bound to any protocol VLAN group.

Command Mode Interface configuration

Usage Guideline The valid interface for this command can be either a physical port or a port-channel.

Use the **dot1v binding protocol-group** command to bind a protocol VLAN group with a VLAN ID. As a result, the packet that matches the specified protocol group will be associated with the VLAN binding with this group.

The VLAN does not need to exist for the command to succeed.

If the *GROUP ID* is not specified when using the command **no dot1v binding protocol-group**, the switch will remove all the protocol group and VLAN bindings at the specified interface.

Example This example shows how to bind a protocol VLAN group 10, VLAN id 3000 of ethernet port 3.2

```
Switch(config)# interface eth3.2
Switch(config-if)# dot1v binding protocol-group 10 vlan 3000
```

Verify the settings by entering the **show dot1v interface** command.

dot1v protocol-group

Use the **dot1v protocol-group** global configuration command to add a protocol to a protocol group. Use no command to remove the specified protocol group, or to remove a protocol VLAN from the specified group.

dot1v protocol-group *GROUP-ID* **frame { ethernet2 | snap | llc }** *TYPE-VLAUE*

no dot1v protocol-group *GROUP-ID* **[frame { ethernet2 | snap | llc }** *TYPE-VLAUE* **]**

Syntax Description	
GROUP-ID	Specifies the protocol group id to add, delete or configure. The valid GROUPID range is 1 to 16.
frame	Specifies frame type to be bound in this entry.
ethernet2	Specifies operational protocol value of Ethernet II type frames.
snap	Specifies operational protocol value of SNAP type frames.
llc	Specifies operational protocol value of LLC type frames.
TYPE-VLAUE	Specifies the protocol value of the specific frame type. The value is in hexadecimal form. Range is 0x0 to 0xFFFF.

Default The default protocol VLAN table is empty.

Command Mode Global configuration

Usage Guideline The **dot1v protocol-group** command adds a protocol to a protocol group.

By setting the command multiple times, multiple protocols can be added to the same group.

The **no dot1v protocol-group** command will delete an existing protocol VLAN group.

If a specific protocol is specified with the no command, then this specific protocol will be removed from the specified group.

Example This example shows how to create a protocol VLAN group with id 10, and bind protocol IPv6 (frame type is ethernet2 value is 0x86dd).

```
Switch(config)# dot1v protocol-group 10 frame ethernet2 0x86dd
```

Verfiy the settings by entering the **show dot1v protocol-group** command.

dot1x auth-mode

Use the **dot1x auth-mode** command to specify the 802.1x authentication mode.

dot1x auth-mode {port-based | host-based}

Syntax Description	
port-based	Specifies the authentication mode as port-based. When in the port-based mode if one supplicant is successfully authenticated, other hosts that are connected to the same port are allowed to access the port. Each port implements one authenticator state machine.
host-based	Specifies the authentication mode as host-based. When in the host-based mode, each host is identified by its MAC address. Only hosts which are successfully authenticated are allowed to access the port. Each MAC address implements one authenticator state machines.

Default **port-based mode**

Command Mode Interface configuration

Usage Guideline The maximum number of hosts allowed to connect to an 802.1X-enabled port is project-dependent.

Example The following example shows how to specify the authentication mode as host-based.

```
Switch(config)#interface eth4.3
Switch(config-if)# dot1x auth-mode host-based
```

Verify the settings by entering the **show dot1x auth-configuration** command.

dot1x auth-protocol

Use this command to specify the authentication method used for 802.1x authentication.

dot1x auth-protocol {local | radius}

Syntax Description	
local	Specifies local accounts for authentication
radius	Specifies RADIUS servers for authentication

Default **radius**

Command Mode Global configuration

Usage Guideline If **local** is specified, a user account should be configured. Please refer to the **dot1x user command on page 175** to create new user accounts.

If **radius** is specified, a RADIUS server should be configured for authentication. Please refer to the **server command on page 526** in **"AAA Feature Commands" on page 1**.

Example The following example shows how to specify the authentication method as RADIUS.

```
Switch# configure terminal
Switch(config)# dot1x auth-protocol radius
```

Verify the settings by entering the **show dot1x command on page 577**.

dot1x control-direction

Use this command to configure the direction of the traffic on a controlled port as unidirectional (**in**) or bidirectional (**both**).

dot1x control-direction { both | in }

Syntax Description	
both	Enable bidirectional control. Both incoming and outgoing traffic through an 802.1X-enabled port are blocked if the port is not successfully authenticated.
in	Enable unidirectional control. Incoming traffic through an 802.1X-enabled port is blocked if the port is not successfully authenticated.

Default **both**

Command Mode Interface configuration

Usage Guideline This command is only valid for physical port interface.

This command takes effect only when the global and per-port 802.1x enable command is configured.

When the port is in force-unauthorized or un-authorized state, the traffic direction is controlled based on this command.

When the port is in force-authorized or authorized state, the traffic is allowed in both directions.

Example The following example shows how to specifies the direction of the traffic through port eth4.1 as unidirectional.

```
Switch# configure terminal
Switch(config)# interface eth4.1
Switch(config-if)# dot1x control-direction in
```

Verify the settings by entering the **show dot1x auth-configuration** command.

dot1x default

Using this command resets the configurable 802.1X parameters to the default values.

dot1x default

Syntax None

Default The default values are listed as following:

The authorization state on a controlled port is auto.

The direction of the traffic through a controlled port is bidirectional.

The number of maximum retransmit times which the switch will retransmit an EAP request frame to the supplicant before restarting the authentication process is 2.

The quiet-period, reauth-period, server-timeout, supp-timeout, and tx-period are 60, 3600, 30, 30, and 30 seconds, respectively.

Periodic re-authentication is disabled.

Command Mode Interface configuration

Usage Guideline This command is only valid on physical port interface.

Example The following example shows how to reset the IEEE 802.1X parameters on port eth4.1.

```
Switch# configure terminal
Switch(config)# interface eth4.1
Switch(config-if)# dot1x default
```

Verify the settings by entering the **show dot1x auth-configuration** command.

dot1x forward-pdu

Use this command to allow a 1X-disabled interface to forward 802.1X BPDU. Use the no form of this command to disable the forwarding function on a 1X-disabled interface.

dot1x forward-pdu

no dot1x forward-pdu

Syntax None

Default 802.1x BPDU is not forwarded when 802.1x is disabled.

Command Mode Interface configuration

Usage Guideline This command is only valid for physical port interface.

When the 802.1X functionality is disabled, and dot1x forward-pdu is configured for a port, the received 1x BPDU on the port will be flooded to the ports where forward-pdu is enabled and that are in the same VLAN.

Example This example shows how to enable 802.1X forward-pdu on a given interface.

```
Switch# configure terminal
Switch(config)# interface eth4.1
Switch(config-if)# dot1x forward-pdu
```

Verify the settings by entering the **show dot1x auth-configuration** command.

dot1x guest-vlan

Use this command to enable the 802.1X guest VLAN function and specify the guest VLAN. Use the no form of this command to disable the guest VLAN function.

dot1x guest-vlan *VLAN-ID*

no dot1x guest-vlan

Syntax None

Default Disabled

Command Mode Interface configuration

Usage Guideline This command is only valid for physical port interfaces.

The guest VLAN is not supported in host-based mode.

The guest VLAN is only effective when a port is configured as 1X-enabled and dot1x port-control is in auto mode.

This command only supports ports in access VLAN mode. When configuring a guest VLAN for a port in other VLAN modes, an error messages appears.

The VLAN assignment of the guest VLAN is determined by following rules:

- If the guest VLAN is enabled, and the authentication state is unauthorized, the port belongs to the guest VLAN.
- If the guest VLAN is enabled with the authentication state authorized, and if RADIUS is authorizing VLAN access then the configured port will belong to the VLAN assigned by RADIUS server, else the port belong to the VLAN configured in the VLAN module.
- If guest VLAN is disabled, and the authentication state is unauthorized, the port belongs to the VLAN configured in VLAN module.
- If guest VLAN is disabled, with the authentication state authorized, and if RADIUS is authorizing VLAN access then the configured port will belong to the VLAN assigned by RADIUS server, else the port belong to the VLAN configured in the VLAN module.
- For a port configured for guest VLAN or RADIUS assigned VLAN, if the configured VLAN is not existing on the switch, the port will belong to the VLAN configured in VLAN module.

Examples The example, on the next page, shows how to make eth4.1 join the IEEE 802.1x guest VLAN.

```
Switch# configure terminal
Switch(config)# interface eth4.1
Switch(config-if)# dot1x guest-vlan 99
```

This example shows how to make eth4.1 leave the guest VLAN.

```
Switch# configure terminal
Switch(config)# interface eth4.1
Switch(config-if)# no dot1x guest-vlan
```

Verify the settings by entering **show do1x auth-configuration** and **show vlan interface** command.

dot1x initialize

Use this command to initialize the authentication state machine of:

- a port in port-based mode.

  -or-

- an associated MAC address in host-based mode.

dot1x initialize [interface *INTERFACE-ID* **[mac-address** *MAC-ADDRESS* **]]**

Syntax Description	
interface *INTERFACE-ID*	(Optional) Specifies a physical interface to initialize. In port-based mode, initialize the authenticator state machine of a port. In host-based mode, initialize all authenticator state machines of associated MAC addresses on this port.
mac-address *MAC-ADDRESS*	(Optional) Specifies a MAC address to initialize. This option is valid only in host-based mode. Will initialize the authenticator state machine of this assigned MAC address on a specific port.

Default None

Command Mode Privileged EXEC

Usage Guideline Entering **dot1x initialize** without any keyword will initialize all authentication states for all ports in port-based mode, or all MAC addresses associated in host-base mode.

Examples This example shows how to initialize the authentication state machine on eth4.1.

```
Switch# dot1x initialize interface eth4.1
```

This example shows how to initialize the authentication state machine associated with MAC address 00-40-10-28-19-78 on eth4.1.

```
Switch# dot1x initialize interface eth4.1 mac-address 00-40-10-28-19-78
```

dot1x max-req

Use this command to set the maximum number of times that the switch sends EAP-request/identity frames to the client before restarting the authentication process.

dot1x max-req *TIMES*

Syntax Description	
max-req *TIMES*	Number of times that the switch retransmits an EAP frame to the client before restarting the authentication process. The range is 1 to 10.

Default *TIMES*: 2

Command Mode Interface configuration

Usage Guideline This command is only valid for physical port interface.

Example This example shows how to set the maximum number of retransmit times on port eth4.1 to be 3.

```
Switch# configure terminal
Switch(config)# interface eth4.1
Switch(config-if)# dot1x max-req 3
```

Verify the settings with the **show dot1x auth-configuration** command.

dot1x pae authenticator

Use this command to enable 802.1X authentication on a specific port. Use the no form of this command to disable 802.1X authentication on the port.

dot1x pae authenticator

no dot1x pae

Syntax Description	
authenticator	Enable 802.1X authentication on a specific port.

Default Disabled

Command Mode Interface configuration

Usage Guideline This command is only valid for physical port interface.

Use the **dot1x system-auth-control command on page 173** to enable global 802.1x function before enabling 802.1X authentication on a specific port.

A port can be configured as a 1x-enable port only if the port is not a member port of a port channel, or a destination port of a port mirroring session.

Examples This example shows how to configure port eth4.1 as a 1X-enabled port.

```
Switch# configure terminal
Switch(config)# interface eth4.1
Switch(config-if)# dot1x pae authenticator
```

This example shows how to disable 802.1x authentication on port eth4.1.

```
Switch# configure terminal
Switch(config)# interface eth4.1
Switch(config-if)# no dot1x pae
```

dot1x port-control

Use this command to manually control the authorization state on a specific port.

dot1x port-control { auto | force-authorized | force-unauthorized }

Syntax Description	
auto	The state (authorized or unauthorized) for a specific port is determined according to the outcome of the authentication.
force-authorized	Specifies to force the port to change to the authorized state. The port allows access and all authentication packets are ignored.
force-unauthorized	Specifies to force the port to change to the unauthorized state. The port is blocked and all authentication packets are ignored.

Default **auto**

Command Mode Interface configuration

Usage Guideline This command is valid only for physical port interface.

Global 802.1x authentication function should be enabled using the **dot1x system-auth-control command on page 173** before enabling 802.1X authentication on a specific port.

Example This example shows how to deny all access on eth4.1.

```
Switch# configure terminal
Switch(config)# interface eth4.1
Switch(config-if)# dot1x port-control force-unauthorized
```

Verify the settings with the **show dot1x auth-configuration** command.

dot1x re-authenticate

Use this command to re-authenticate a specific port or a specific MAC address.

dot1x re-authenticate [interface *INTERFACE-ID* **[mac-address** *MAC-ADDRESS* **]]**

Syntax Description	
interface *INTERFACE-ID*	(Optional) Specifies a port to re-authenticate. This option is only valid for physical port interface.
mac-address *MAC-ADDRESS*	(Optional) Specifies a MAC address to re-authenticate. This option can be used only in host-based mode.

Default None

Command Mode Privileged EXEC

Usage Guideline Entering **dot1x re-authenticate** without any keyword will re-authenticate all 1x-enabled ports in the port-based mode or all MAC addresses associated with 1x-enabled port in the host-based mode.

Examples This example shows how to re-authenticate eth4.1.

```
Switch# dot1x re-authenticate interface eth4.1
```

This example shows how to re-authenticate MAC address 00-40-10-28-19-78 on eth4.1.

```
Switch# dot1x re-authenticate interface eth4.1 mac-address 00-40-10-28-19-78
```

dot1x re-authentication

Use this command to enable periodic re-authentication. Use the no form of this command to disable periodic re-authentication.

dot1x re-authentication

no dot1x re-authentication

Syntax None

Default Disabled

Command Mode Interface configuration

Usage Guideline This command is valid only for physical port interface.

The number of seconds between re-authentication attempts can be configured using the **dot1x timeout command on page 174** with the **reauth-period** keyword**.**

Examples This example enables periodic re-authentication on eth4.1.

```
Switch# configure terminal
Switch(config)# interface eth4.1
Switch(config-if)# dot1x re-authentication
```

This example shows how to disable periodic-re-authentication.

```
Switch# configure terminal
Switch(config)# interface eth4.1
Switch(config-if)# no dot1x re-authentication
```

Verify the settings by entering the **show dot1x auth-configuration** command.

dot1x system-auth-control

Use **dot1x system-auth-control** to globally enable 802.1X authentication on a switch. Use the no form of this command to return to globally disable 802.1X function.

dot1x system-auth-control

no dot1x system-auth-control

Syntax None

Default Disabled

Command Mode Global configuration

Usage Guideline None

Examples This example shows how to globally enable 802.1X authentication on a switch.

```
Switch# configure terminal
Switch(config)# dot1x system-auth-control
```

This example shows how to disable 802.1x authentication globally on a switch.

```
Switch# configure terminal
Switch(config)# no dot1x system-auth-control
```

Verify the settings by entering the **show dot1x auth-configuration** command.

dot1x timeout

Use this command to set timeout values for various 802.1X timers.

dot1x timeout {quiet-period *SECONDS* **| reauth-period** *SECONDS* **| server-timeout** *SECONDS* **| supp-timeout** *SECONDS* **| tx-period** *SECONDS* **}**

Syntax Description	
quiet-period *SECONDS*	Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 0 to 65535.
reauth-period *SECONDS*	Number of seconds between re-authentication attempts. The range is 1 to 65535
server-timeout *SECONDS*	Number of seconds that the switch will wait when it does not receive notification from the authentication server. The range is 1 to 65535.
supp-timeout *SECONDS*	Number of seconds that the switch will wait when it does not receive any notification from the client. The range is 1 to 65535.
tx-period *SECONDS*	Number of seconds that the switch waits for a response to an EAP-request/ identity frame from the client before retransmitting the request. The range is 1 to 65535.

Default

quiet-period: 60 seconds

reauth-period:3600 seconds

server-timeou: 30 seconds

supp-timeout: 30 seconds

tx-period: 30 seconds

Command Mode

Interface configuration

Usage Guideline

This command is only valid for physical port interface.

The r**eauth-period** takes effect when re-authentication is configured by the **dot1x re-authentication command on page 172**.

Example

This example sets **quiet-period**, **reauth-period**, **server-timeout**, **supp-timeout**, and **tx-period** on eth4.1 to be 20, 1000, 15, 15, and 10 seconds, respectively.

```
Switch# configure terminal
Switch(config)# interface eth4.1
Switch(config-if)# dot1x timeout quiet-period 20
Switch(config-if)# dot1x timeout reauth-period 1000
Switch(config-if)# dot1x timeout server-timeout 15
Switch(config-if)# dot1x timeout supp-timeout 15
Switch(config-if)# dot1x timeout tx-period 10
```

Verify the settings by entering the **show dot1x auth-configuration** command.

dot1x user

Use this command to create a local account used for authentication. Use the no form of this command to delete local accounts.

dot1x user *NAME* **password** *PASSWORD*

no dot1x user [*NAME* **]**

Syntax Description	
NAME	Specifies the name of a local account used for authentication. The valid length is from 1 to 32. The syntax is general string that does not allow space.
password *PASSWORD*	Specifies a password for a local account. The valid length is from 1 to 16. The syntax is general string that does not allow space.

Default No local account is created.

Command Mode Global configuration

Usage Guideline All accounts can be removed by entering **no dot1x user** without the *NAME* option.

The local database can be used in both port-based and host-based mode.

The maximum number of user accounts is project dependent.

Examples This example creates a local account with username. "yourname" and password "yourpass".

```
Switch# configure terminal
Switch(config)# dot1x user yourname password yourpass
```

This example deletes a local account with a username as "yourname".

```
Switch# configure terminal
Switch(config)# no dot1x user yourname
```

Verify the settings by entering the **show dot1x user** command.

duplex

Use this command to configure the physical port interface speed/duplex setting.

duplex { full | half | auto }

Syntax Description	
full	Specifies to operate in full duplex mode.
half	Specifies to operate in half duplex mode.
auto	Specifies that the duplex mode will be determined by auto-negotiation.

Default **auto**

Command Mode Interface configuration

Usage Guideline Physical port interfaces are valid for this configuration. If the duplex mode is not supported by the hardware, an error message will be returned.

The following hardware restrictions apply:

- 1000SX/LX is always fixed to 1000 and full duplex.
- 100FX is always fixed 100 and full duplex.
- For all SFP/XFP modules,the duplex command will not take any effect.

Auto-negotiation is enabled if either for speed or duplex. If speed is set to auto, and duplex is set to full or half mode, then only the speed will be negotiated. The advertised capability will be the configured duplex mode combined with all possible speeds. If speed is to set to a fixed speed and duplex is set to auto, then only duplex mode is negotiated. The advertised capability will be both full and half duplex mode combined with the configured speeds.

Before adding ports to a Port-Channel, please verify that all settings are identical on the candidate ports; otherwise the port members of a Port-Channel with different settings will operate in an indeterminate manner.

Example This example shows how to configure interface eth3.1 to force the settings to a speed of 100Mbits and auto-negotiate to the duplex mode.

```
Switch(config)# interface eth3.1
Switch(config-if)# speed 100
Switch(config-if)# duplex auto
```

Verify the settings by entering the **show interface** command.

enable

Use this command to enter a Privileged EXEC mode.

enable [privilege LEVEL]

Syntax Description	
privilege *LEVEL*	(Optional) Sets the privilege level for the user. The privilege levels are 12 and 15.

Default *LEVEL:* 15

Command Mode User EXEC

Usage Guideline Use the enable command to enter the Privileged EXEC mode and use the **disable command on page 150** to return to the User EXEC mode from the power user level.

The command only accepts level 12 and 15.

An error message will appear if other levels are specified.

If the enable password is configured for a level, the user will be requested to enter the password for the specified privileged level.

Example This example shows how to enter the Privileged EXEC mode:

```
Switch> enable
Input privileged level 15 password:
Switch#
```

enable password

Use this command to setup the enable password to enter into different privileged modes. Use the no form of the command to return the password for all levels to an empty string. When a level is specified, the password for that level is returned to an empty string.

enable password privilege *LEVEL* **password {plain-text| encrypted }** *PASSWORD*

no enable password [privilege *LEVEL***]**

Syntax Description	
privilege *LEVEL*	Sets the privilege level the password will protect. The privilege level is either 12 or 15. If this argument is not specified in the command or in the no form of the command, the privilege level defaults to 15 (the traditional enable privileges).
plain-text *PASSWORD*	Specifies the password the user must enter to gain access to the switch. The password must be from 6 to 32 characters (the length of password in plain-text form may be project-dependant) and can contain embedded spaces. The password is case-sensitive. The syntax is a general string that allows spaces.
encrypted *PASSWORD*	Specifies the password in the encrypted form based on SHA-I. For the encrypted form of the password, the length is fixed to 35 bytes long. The password is case-sensitive. Using the **show username** or **show enable password** command, an encrypted password can be copied and pasted to this command option.

Default No enable password is configured.

Command Mode Global configuration at privilege level 15

Usage Guideline Only accepts level 12 and 15.

An error message will appear if other levels are specified.

The exact password for the specific level needs to be used in order to enter the specific level of the privileged EXEC mode.

Each level has only one password in order to enter that level.

Example This example shows how to create an enable password for privilege level 15 with "MyEnablePassword".

```
Switch(config)# enable password MyEnablePassword
```

Verify the settings by entering the **show enable password** command.

end

Use this command to end the current configuration session and go back to the Privileged EXEC mode.

end

Syntax None

Default None

Command Mode Any configuration mode

Usage Guideline Using this command will end the configuration task in any configuration mode and go back to the Privileged EXEC mode.

If the current mode in any of the EXEC mode, this command will logout the session.

Example This example shows how to end the interface configuration and go back to privileged mode.

```
Switch(config-if)#end
Switch#
```

exit

Use this command to end the current configuration mode and go back to the to the last mode used.

exit

Syntax None

Default None

Command Mode Any

Usage Guideline The user can exit the current configuration mode and go back to the last mode used.

When the user is in User EXEC mode, this command will logout the session.

Example This example shows how to exit from the interface configuration mode and return to the global configuration mode.

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

erps

Use the erps command to enable ERPS function globally. Use the no form of this command to disable ERPS function globally.

erps

no erps

Syntax None

Default Disabled

Command Mode Global configuration mode

Usage Guideline Enable ERPS function globally will also enable all ERP instances which state are enabled by using "erpi enable" command. And, disable ERPS function globally will disable all ERP instances.

Example The following example shows how to enable ERPS function globally:

```
Switch(config)# erps
Switch(config)#
```

The following example shows how to disable ERPS function globally:

```
Switch(config)# no erps
Switch(config)#
```

erps domain

Use the erps domain command to create or modify an ERPS domain and enter the ERPS domain configuration mode. Use the no form of this command to delete an ERPS domain.

erps domain *DOMAIN-NAME*

no erps domain *DOMAIN-NAME*

Syntax Description	
DOMAIN-NAME	Specifies the name of ERPS domain with a maximum of 32 characters. (Only allow character set: '0-9', 'a-z', 'A-Z', '-').

Default No ERPS domain is created.

Command Mode Global configuration mode

Usage Guideline Use the erps domain command to create or modify an ERPS domain and enter the ERPS domain configuration mode.

Example The following example shows how to create ERPS domain campus:

```
Switch(config)# erps domain campus
Switch(config-erps-domain)#
```

The following example shows how to delete ERPS domain campus:

```
Switch(config)# no erps domain campus
Switch(config)#
```

erpi enable

Use the erpi enable command to enable the ERP instance in an ERPS domain. Use the no form of this command to disable the ERP instance.

erpi *INSTANCE-ID* **enable**

no erpi *INSTANCE-ID* **enable**

Syntax Description	
INSTANCE-ID	Specifies the identifier of ERP instance. The vlaid range is 1 to 4095.

Default Disabled

Command Mode ERPS domain configuration mode

Usage Guideline Use the command to enable the administrative state of an EPR instance. The R-APS VLAN, ring ports, RPL setting must be configured first before the ERP instance can be enabled.

The command does not take effect under the following conditions. The ERP instance is still in operational disabled state.

1.The configured R-APS controlled VLAN does not exist.

2.The configured ring ports are not the tag member port of the R-APS controlled VLAN.

In addition to R-APS controlled VLAN and ring ports, the configuration of service protected VLANs and RPL related settings are fundamental for the setup of an ERP instance.

Example The following example shows how to enable ERP instance 1 in ERPS domain campus:

```
Switch(config)# erps domain campus
Switch(config-erps-domain)# erpi 1 enable
Switch(config-erps-domain)#
```

The following example shows how to disable ERP instance 1 in ERPS domain campus:

```
Switch(config)# erps domain campus
Switch(config-erps-domain)# no erpi 1 enable
Switch(config-erps-domain)#
```

erpi type

Use the erpi type command to create an ERP instance with ring type in an ERPS domain. Use the no form of this command to delete an ERP instance.

erpi *INSTANCE-ID* **type {major | sub}**

no erpi *INSTANCE-ID*

Syntax Description	
INSTANCE-ID	Specifies the identifier of the ERP instance. The valid range is 1 to 4095.
major	Specifies the ring as a major-ring.
sub	Specifies the ring as a sub-ring.

Default No ERP instance is created.

Command Mode ERPS domain configuration mode

Usage Guideline Use the erpi type command to create an ERP instance before doing other configuration for the ERP instance. Use the no erpi command to delete an ERP instance. All configured settings for the ERP instance are thus removed.

An ERPS domain can contain multiple ERP instances. Generally, the instances in the same domain protect the same set of VLANs or the set of VLANs protected by one instance is a subset of the set of VLANs protected by another instance.

If multiple ERP instances are configured, then one of them should be the major instance and the rest of them are sub instances.

The ID of ERP instances in different domains are global significant.

To change the type of an instance, remove the instance first and re-create the instance.

Example The following example shows how to create ERP instance 1 as the major ring:

```
Switch(config-erps-domain)# erpi 1 type major
Switch(config-erps-domain)#
```

The following example shows how to create ERP instance 2 as a sub ring:

```
Switch(config-erps-domain)# erpi 2 type sub
Switch(config-erps-domain)#
```

The following example shows how to delete ERP instance 1:

```
Switch(config-erps-domain)# no erpi 1
Switch(config-erps-domain)#
```

erpi raps-vlan

Use the erpi raps-vlan command to configure the R-APS controlled VLAN of an ERP instance. Use the no form of this command to remove the R-APS controlled VLAN setting.

erpi *INSTANCE-ID* **raps-vlan** *VLAN-ID*

no erpi *INSTANCE-ID* **raps-vlan**

Syntax Description	
INSTANCE-ID	Specifies the identifier of ERP instance. The valid range is 1 to 4095.
VLAN-ID	Specifies the VLAN ID of RAPS controlled VLAN for the ERP instance. The valid range is 1 to 4094.

Default Not configured

Command Mode ERPS domain configuration mode

Usage Guideline Use the command to assign the R-APS controlled VLAN for the ERP instance. The R-APS controlled VLAN need to be assigned before the ERP instance can be enabled.

The specified R-APS VLAN does not need to exist to configure the command.

If user removes the R-APS controlled VLAN when the ERP instance is in operation, the ERP instance will enter operational disabled state.

Different ERP instances can not use the same R-APS controlled VLAN.

Example The following example shows how to configure R-APS controlled VLAN to "2" of ERP instance 1:

```
Switch(config-erps-domain)# erpi 1 raps-vlan 2
Switch(config-erps-domain)#
```

The following example shows how to remove R-APS controlled VLAN setting of ERP instance 1:

```
Switch(config-erps-domain)# no erpi 1 raps-vlan
Switch(config-erps-domain)#
```

erpi ring-mel

Use the erpi ring-mel command to configure ring MEL value of an ERP instance. Use the no form of this command to return to default setting.

erpi *INSTANCE-ID* **ring-mel** *MEL-VALUE*

no erpi *INSTANCE-ID* **ring-mel**

Syntax Description	
INSTANCE-ID	Specifies the identifier of the ERP instance. The valid range is 1 to 4095.
MEL-VALUE	Specifies the ring MEL value of the ERP instance. The valid range is 0 to 7.

Default 1

Command Mode ERPS domain configuration mode

Usage Guideline The configured ring MEL value for all ring nodes of an ERP instance should be the same.

Example The following example shows how to configure ring MEL value to "6" of ERP instance 1:

```
Switch(config-erps-domain)# erpi 1 ring-mel 6
Switch(config-erps-domain)#
```

The following example shows how to return ring MEL value to default value of ERP instance 1:

```
Switch(config-erps-domain)# no erpi 1 ring-mel
Switch(config-erps-domain)#
```

erpi ring-port

Use the erpi ring-port command to configure the ring ports of an ERP instance. Use the no form of this command to remove the ring port setting.

erpi *INSTANCE-ID* **ring-port {east | west} {shared |** *INTERFACE-ID***}**

no erpi *INSTANCE-ID* **ring-port {east | west | shared}**

Syntax Description	
INTERFACE-ID	Specifies the identifier of the ERP instance. The valid range is 1 to 4095.
east	Specifies the port as the east ring port.
west	Specifies the port as the west ring port.
shared	Specifies the port as a shared ring port for the sub ERP instance.
INTERFACE-ID	Specifies the interface of configured ring port, it can be a physcial port or a port-channel interface.

Default Not configured

Command Mode ERPS domain configuration mode

Usage Guideline Use the command to configure the ring ports for the ERP instance. For each ERP instance, two ring ports, east ring port and west ring port need to be configured.

The ring port should be configured as the tag member ports of the R-APS controlled VLAN.

Example The following example shows how to configure interface "eth3.1" as the east ring port of ERP instance 1:

```
Switch(config-erps-domain)# erpi 1 ring-port east eth3.1
Switch(config-erps-domain)#
```

The following example shows how to configure interface "eth3.2" as the west ring port of ERP instance 1:

```
Switch(config-erps-domain)# erpi 1 ring-port west eth3.2
Switch(config-erps-domain)#
```

The following example shows how to configure interface "port-channel1" as the east ring port of ERP instance 1:

```
Switch(config-erps-domain)# erpi 1 ring-port east port-channel1
Switch(config-erps-domain)#
```

The following example shows how to remove east ring port setting of ERP instance 1:

```
Switch(config-erps-domain)# no erpi 1 ring-port east
Switch(config-erps-domain)#
```

The following example shows how to configure east ring port to shared ring port of ERP instance 2 (sub ERP instance)

```
Switch(config-erps-domain)# erpi 2 ring-port east shared
Switch(config-erps-domain)#
```

The following example shows how to remove shared ring port of ERP instance 2 (sub ERP instance)

```
Switch(config-erps-domain)# no erpi 2 ring-port shared
Switch(config-erps-domain)#
```

erpi rpl

Use the erpi rpl command to configure an ERP instance as the RPL owner and the RPL port. Use the no form of this command to remove the RPL related setting.

erpi *INSTANCE-ID* **rpl owner rpl-port {east | west }**

no erpi *INSTANCE-ID* **rpl**

Syntax Description	
INSTANCE-ID	Specifies the identifier of ERP instance. The valid range is 1 to 4095.
owner	Specifies the ring node as the RPL owner of the ERP instance.
rpl-port	Specifies one of the ring ports as the RPL port.

Default Not configured

Command Mode ERPS domain configuration mode

Usage Guideline Use the command to specify one of the nodes in the ring as the RPL owner, and one of its ring ports as the RPL port.

The setup of the RPL owner and RPL port are required for operation of the ring.

Example The following example shows how to enable RPL owner and configure RPL port to east ring port of ERP instance 1:

```
Switch(config-erps-domain)# erpi 1 rpl owner rpl-port east
Switch(config-erps-domain)#
```

The following example shows how to enable RPL owner and configure RPL port to west ring port (non-shared) of ERP instance 2:

```
Switch(config-erps-domain)# erpi 2 rpl owner rpl-port west
Switch(config-erps-domain)#
```

The following example shows how to disable RPL owner of ERP instance 1:

```
Switch(config-erps-domain)# no erpi 1 rpl
Switch(config-erps-domain)#
```

erpi protected-vlan

Use the erpi protected-vlan command to add or remove service protected VLANs for an ERP instance. Use the no form of this command to remove all service protected VLANs.

erpi *INSTANCE-ID* **protected-vlan {***VLAN-ID* **[,|-] | add** *VLAN-ID* **[,|-] | remove** *VLAN-ID* **[,|-]}**

no erpi *INSTANCE-ID* **protected-vlan**

Syntax Description	
INSTANCE-ID	Specifies the identifier of the ERP instance. The valid range is 1 to 4095
VLAN-ID	Specifies the VLAN ID of the service protected VLANs of the ERP instance. The valid range is 1 to 4094.

Default Not configured

Command Mode ERPS domain configuration mode

Usage Guideline Use the command to configure the VLANs to be protected by the ERP instance.

The user should assign the service protected VLANs that are distinguished from the R-APS control VLAN of all created ERP instances.

If an ERPS domain contains multiple ERP instances, generally, the VLANs protected by them should be consistent.

Example The following example shows how to configure service protected VLAN as 3 of ERP instance 1:

```
Switch(config-erps-domain)# erpi 1 protected-vlan 3
Switch(config-erps-domain)#
```

The following example shows how to add service protected VLANs "4-6" of ERP instance 1:

```
Switch(config-erps-domain)# erpi 1 protected-vlan add 4-6
Switch(config-erps-domain)#
```

The following example shows how to add service protected VLANs "7,9" of ERP instance 1:

```
Switch(config-erps-domain)# erpi 1 protected-vlan add 7,9
Switch(config-erps-domain)#
```

The following example shows how to remove service protected VLAN "3" of ERP instance 1:

```
Switch(config-erps-domain)# erpi 1 protected-vlan remove 3
Switch(config-erps-domain)#
```

The following example shows how to remove all service protected VLANs of ERP instance 1:

```
Switch(config-erps-domain)# no erpi 1 protected-vlan
Switch(config-erps-domain)#
```

erpi timer

Use the erpi timer command to configure timers for an ERP instance. Use the no form of this command to reset timer to default value.

erpi *INSTANCE-ID* **timer [guard** *MILLI-SECONDS***] [hold-off** *MILLI-SECONDS***] [wtr** *MINUTES***]**

no erpi *INSTANCE-ID* **timer [guard] [hold-off] [wtr]**

Syntax Description	
INSTANCE-ID	Specifies the identifier of the ERP instance. The valid range is1 to 4095.
guard *MILLI-SECONDS*	Specifies the guard timer in milliseconds. The valid range is 10 to 2000. The value should be a multiple of 10.
hold-off *MILLI-SECONDS*	Specifies the hold-off timer in milliseconds. The valid range is 0 to 10000. The value should be a multiple of 100.
wtr *MINUTES*	Specifies the WTR timer in minutes. The valid range is 1 to 12.

Default The default guard timer is 500 milliseconds.

The default hold-off timer is 0.

The default WTR timer is 5 minutes.

Command Mode ERPS domain configuration mode

Usage Guideline Use the command to configure timers for the ERP instance

Example The following example shows how to configure guard timer to "600 ms" of ERP instance 1:

```
Switch(config-erps-domain)# erpi 1 timer guard 600
Switch(config-erps-domain)#
```

The following example shows how to configure guard timer to 700 milliseconds, hold-off timer to 100 milliseconds of ERP instance 1:

```
Switch(config-erps-domain)# erpi 1 timer guard 700 hold-off 100
Switch(config-erps-domain)#
```

The following example shows how to configure WTR timer to 1 minutes of ERP instance 1:

```
Switch(config-erps-domain)# erpi 1 timer wtr 1
Switch(config-erps-domain)#
```

The following example shows how to configure hold-off timer as default time value of ERP instance 1:

```
Switch(config-erps-domain)# no erpi 1 timer hold-off
Switch(config-erps-domain)#
```

erpi tc-propagation

Use the erpi tc-propagation command to enable topology change propagation of the sub ERP instance. Use the no form of this command to disable topology change propagation.

erpi *INSTANCE-ID* **tc-propagation**

no erpi *INSTANCE-ID* **tc-propagation**

Syntax Description	
INSTANCE-ID	Specifies rhe identifier of the sub ERP instance. The valid range is 1 to 4095.

Default Disabled

Command Mode ERPS domain configuration mode

Usage Guideline The command setting only takes effect for the sub ERP instance.

Example The following example shows how to enable tc propagation state of sub ERP instance 2 in ERPS domain 1:

```
Switch(config)# erps domain 1
Switch(config-erps-domain)# erpi 2 tc-propagation
Switch(config-erps-domain)#
```

The following example shows how to disable tc propagation state of sub ERP instance 2 in ERPS domain 1:

```
Switch(config)# erps domain 1
Switch(config-erps-domain)# no erpi 2 tc-propagation
Switch(config-erps-domain)#
```

errdisable recovery

Use the **errdisable recovery** command to enable and configure the error recovery function. Use the no command to disable the auto recovery for causes or to return interval to default setting for causes.

errdisable recovery cause {all | loopback-detection } [interval*SECONDS* **]**

no errdisable recovery cause {all | loopback-detection } [interval]

Syntax Description	
all	Specifies the configure auto recovery for all causes.
loopback-detection	Specifies the configure auto recovery of error report caused by **loopback-detection**
interval*SECONDS*	Specifies the time, in seconds, to recover the port from an error state caused by the specified module. The valid value is 30 to 86400.

Default

Auto recovery is disabled for all causes

If enabled, the Interval is 300 seconds

Command Mode

Global configuration

Usage Guideline

A port can be put in error disabled state (an operational state that is similar to the link-down state) by causes such as loopback detection.

A port in error disabled state can not transmit nor receive any packets.

An error disabled port can be either manual recovered or automatically restored by using this command.

The user can enter **shutdown** and then **no shutdown** commands to recover an interface manually from the error-disabled state.

If auto recovery is enabled for a specific cause, the port error disabled by that caused will be auto recovered once the cause have timed out.

Example

This example shows how to set the recovery timer to 200 seconds for port loopback-detection.

```
Switch# configure terminal
Switch(config)# errdisable recovery cause loopback-detection interval 200
Switch(config)# end
```

The following example shows how to enable the auto recovery for loopback-detection.

```
Switch# configure terminal
Switch(config)# errdisable recovery cause loopback-detection

Switch(config)# end
```

You can verify your settings by entering the **show errdisable recovery** command.

flowcontrol

Use this command to configure the flow control capability of the port interface.

flowcontrol [send | receive] { on | off }

Syntax Description	
send	(Optional) Flow control setting for a port sends PAUSE frames
receive	(Optional) Flow control setting for a port receives PAUSE frames
on	Enable a port to send PAUSE frames or process PAUSE frames from remote ports
off	Disable the ability for a port to send or receive PAUSE frames

Default **send**: **off**

receive: **off**

Command Mode Interface configuration

Usage Guideline Only physical port interfaces are valid for this configuration.

The command only assures that either the software configured or the administration state complies with the **flowcontrol** command.

The actual operation of the hardware may prevent the **flowcontrol** command to take effect. This is because flow control capability is determined by both the local port, device and its linked partner instead of just the local setting.

If auto-negotiation is disabled (i.e. the speed and duplex are both set to a non-auto setting), then the final flow-control setting will be determined by the configured flow control setting.

If auto-negotiation is enabled (i.e. the speed or duplex setting is set to auto), the final flow control setting will be based on the negotiated result between local side setting and the partner side setting. The configured flow control setting here is the local side setting.

If no option is selected for the direction, then both **send** and **receive** are applied.

Example This example shows how to turn on the flow control send capability of interface eth3.1.

Verify the settings by entering the show interface command.

```
Switch# configure terminal
Switch(config)# interface eth3.1
Switch(config-if)# flowcontrol send on
Switch(config-if)# end
```

gvrp (Global)

Use the **gvrp interface** command to enable GVRP function globally, and use the **no gvrp** command to disable the GVRP function globally.

gvrp

no gvrp

Syntax None

Default Disabled

Command Mode Global configuration

Usage Guideline None

Example This example shows how to enable the GVRP protocol global state.

```
Switch(config)# gvrp

Switch(config)#
```

Verify the settings by entering the **show gvrp configuration** command.

gvrp (Interface)

Use the **gvrp interface** command to enable GVRP function for a port, and use the **no gvrp** command to disable the GVRP function for a port.

gvrp

no gvrp

Syntax None

Default Disabled

Command Mode Interface configuration

Usage Guideline Use the **gvrp** interface configuration command to enable/disable the GVRP protocol state.

Both physical port and port-channel interfaces are valid for this command. If a physical port is member of a port-channel, then this command should return an error message to indicate it.

The GVRP function cannot be enabled when the interface is at access mode.

Example This example shows how to enable Ethernet eth3.1 GVRP protocol state.

```
Switch(config)# interface eth3.1

Switch(config-if)# gvrp
```

Verify the settings by entering the **show gvrp configuration interface** command.

gvrp advertise (Interface)

Use the **gvrp advertise** command to specify that this VLAN will be advertised out by GVRP protocol. Use **no gvrp advertise** to disable this function.

gvrp advertise [*VLAN-ID* **[, | -]]**

no gvrp advertise [*VLAN-ID* **[, | -]]**

Syntax Description	
VLAN-ID **[, | -]**	(Optional) Specifies a VLAN. The range is 1 to 4094. Specify a single VLAN ID, a range of VLANs separated by a hyphen, or a series of VLANs separated by comma.

Default Advertise

Command Mode Interface configuration

Usage Guideline Use the gvrp advertise interface configuration command to enable the specified VLANs' GVRP advertise function on the specified interface. If no VLAN ID is specified, the advertise function of all VLANs to which the specified interface belongs will be enabled.

Both physical port and port-channel interfaces are valid for this command. If a physical port is member of a port-channel, then this command should return an error message to indicate it.

The GVRP advertise function cannot be enabled when the interface is in access mode.

Example This example shows how to enabled advertise function of VLAN 1000 at interface Ethernet eth4.1.

```
Switch(config)# interface eth4.1
Switch(config-if)# gvrp advertise 1000
```

Verify the settings by entering the **show gvrp configuration** command.

gvrp advertise (VLAN)

Use the **gvrp advertise** command to specify that this VLAN will be advertised out by GVRP protocol. Use **no gvrp advertise** to disable this function.

gvrp advertise

no gvrp advertise

Syntax None

Default Advertise is enabled

Command Mode Config-VLAN configuration

Usage Guideline If a VLAN has been configured to be advertised under the config-VLAN mode, GVRP protocol will advertise this VLAN if it has any member ports. However the command takes effect only in the running configuration, it is not stored in NV-RAM for the next start up configuration. In the interface mode, the command is stored in NV-RAM for next startup system configuration mode.

Example This example shows how to configure VLAN 1000 to be advertised.

```
Switch(config)# VLAN 1000

Switch(config-VLAN)# gvrp advertise
```

Verify the settings by entering the **show gvrp configuration** command.

gvrp dynamic-vlan-creation

Use the **gvrp dynamic-vlan-creation** command to enable dynamic VLAN creation, and use the no form of the command to disable the dynamic VLAN creation function.

gvrp dynamic-vlan-creation

no gvrp dynamic-vlan-creation

Syntax None

Default Disabled

Command Mode Global configuration

Usage Guideline When **gvrp dynamic-vlan-creation** is enabled, and a port learns a new VLAN membership where the VLAN does not exist, the VLAN will be created automatically. Otherwise, the newly learned VLAN will not be created.

Example This example shows how to enable dynamic VLAN creation for GVRP.

```
Switch(config)# gvrp

Switch(config)# gvrp dynamic-vlan-creation
```

Verify the settings by entering the **show gvrp configuration** command.

gvrp forbidden

Use the **gvrp forbidden** command to specify the port as a forbidden member. Use the **no gvrp forbidden** command to remove the port as a forbidden member.

gvrp forbidden

no gvrp forbidden

Syntax None

Default None

Command Mode Interface configuration

Usage Guideline The physical port and port-channel interfaces are both valid for this command. If a physical port is a member of a port-channel, entering the command returns an error message. If multiple interfaces are specified, the command can be executed partially. Error messages are sent if the interfaces fail to execute this command.

When the gvrp forbidden command is configured, all VLANs will be forbidden except the default VLAN (1) of this port.

If some VLANs have already been defined as allowable VLANs for the port, then these VLAN memberships will be removed when issuing the **gvrp forbidden** command. These memberships will not be recovered even when the **no gvrp forbidden** command is applied.

Example This example shows how to set Ethernet eth3.1 as a GVRP forbidden port.

```
Switch(config)# interface eth3.1

Switch(config-if)# gvrp forbidden
```

Verify the settings by entering the **show gvrp configuration interface** command

gvrp timer

Use the **gvrp timer** command to set the GVRP timer value for a port.

gvrp timer { join | leave | leave-all } *TIMER-VALUE*

Syntax Description	
join	Set the timer for joining the group. The unit is hundredths of a second.
leave	Set the timer for leaving a group. The unit is hundredths of a second.
leave-all	Set the time for leaving all groups. The unit is hundredths of a second.
TIMER-VALUE <1-65535>	The timer value in hundredths of a second.

Default **join**: 20

leave : 60

leave-all : 1000

Command Mode Interface configuration

Usage Guideline The value of these parameters must comply to the following rules:

1. LEAVE_TIMER >= 3 * JOIN_TIMER
2. LEAVE_ALL_TIMER > LEAVE_TIMER

Example This example shows how to set the leave-all timer to 5 seconds using the value 500 (hundredths of a second).

```
Switch(config)# interface eth3.1

Switch(config-if)# gvrp timer leave-all 500
```

Verify the settings by entering the **show gvrp configuration** interface command.

help

To display a brief description of the help system, use the **help** command in any command mode.

help

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline The help command provides a brief description of the context-sensitive help system, which functions as follows:

To list all commands available for a particular command mode, enter a question mark (?) at the system prompt.

To obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by a question mark (?). This form of help is called word help, because it lists only the keywords or arguments that begin with the abbreviation entered.

To list the keywords and arguments associated with a command, enter a question mark (?) in place of a keyword or argument on the command line. This form of help is called command syntax help, because it lists the keywords or arguments that apply based on the command, keywords, and arguments that have already been entered.

Example In the following example, the help command is used to display a brief description of the help system:

```
Switch# help

The switch CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
```

host area

Use the **host area** command to configure a stub host entry belonging to a particular area. Use the no form of this command to remove the host area configuration.

host *IP-ADDRESS* **area** *AREA-ID* **[cost** *COST* **]**

no host *IP-ADDRESS* **area** *AREA-ID*

Syntax Description	
IP-ADDRESS	Specifies IP address of the host.
AREA-ID	Specifies the identifier of the area for which authentication is to be enabled. The identifier can be specified as either an IP address or a decimal value (4 octets unsigned integer value).
COST	Specifies cost for stub host entry. The range is 0 to 65535.

Default No host entry is configured.

Command Mode Router configuration

Usage Guideline Using this command, specific host routes can be advertised in the router-LSA as stub link.

Example This following example shows how to configure a stub host 172.16.10.100 at area 1.

```
Switch# configure terminal
Switch (config)# router ospf
Switch (config-router)# host 172.16.10.100 area 1
```

Verify the settings by entering the **show ip ospf host-route** command.

hybrid vlan VLAN-ID

Use the **hybrid VLAN** command to set the VLAN characteristic. It sets the interface as a tagged member or untagged member.

hybrid vlan *VLAN-ID* **[, | -] { tagged | untagged }**

no hybrid vlan [*VLAN-ID* **[, | -]]**

Syntax Description	
VLAN-ID	Specifies the VLAN to add or remove tagging member from it.
tagged	Specifies the port as a tagged member of specified VLAN(s).
untagged	Specifies the port as an untagged member of specified VLAN(s).
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specifies a range of VLANs. Enter a space before and after the hyphen.

Default The default hybrid-vlan is empty.

Command Mode Interface configuration

Usage Guideline Physical ports or port-channels are valid interfaces for this command.

By setting the hybrid VLAN command multiple times, a port can be a tagged member port or an untagged member port of multiple VLANs.

If the VLAN does not exist, an error message is returned.

When this command is applied, the port will change to hybrid mode. If the mode is changed, the setting for the previous mode will disappear.

If a VLAN has already been defined as a tagged VLAN, applying this command in untagged VLAN mode will remove that membership.

If a VLAN has already been defined as a un-tagged VLAN, applying this command in tagged VLAN mode will remove that membership.

When using the **no hybrid vlan** command without specifying a VLAN ID, then the port's membership will be removed from all VLANs.

Example This example shows how to set an interface port 3.1 as a tagged member of VLAN 1000.

```
Switch(config)# interface eth3.1
Switch(config-if)# hybrid vlan 1000 tagged
```

Verify the settings by entering the **show vlan** command.

ingress-checking

Use the **ingress-checking** to enable ingress frame checking at a port. Use the **no ingress-checking** to disable the ingress frame checking function.

ingress-checking

no ingress-checking

Syntax None

Default Enabled

Command Mode Interface configuration

Usage Guideline The valid interfaces for this command are physical ports.

Use the **ingress-checking** interface command to enable ingress checking at the switch interfaces. When ingress checking is enabled, if the port is not a member port of the VLAN associated with the incoming frames, the frames will be dropped. Use the **no ingress-checking** interface command to disable this function of a port.

Example This example shows how to set ingress checking to enabled at ethernet port 4.1.

```
Switch(config)# interface eth4.1
Switch(config-if)# ingress-checking
```

Verify the settings by entering the **show vlan interface** command.

instance

To map a VLAN or a set of VLANs to a single Multiple Spanning Tree (MST) instance, use the **instance** command. To return the VLANs to the default instance (CIST), use the no form of this command.

instance *INSTANCE-ID* **vlans** *VLANDID* **[, | .]**

no instance *INSTANCE-ID*

Syntax Description	
INSTANCE-ID	Instance to which the specified VLANs are mapped; valid values are from 1 to 63.
vlans *VLANDID* **[** , | .**]**	Specifies the number of the VLANs to be mapped to the specified instance; valid values are from 1 to 4094.

Default No VLANs are mapped to any MST instance (all VLANs are mapped to the CIST instance).

Command Mode MST configuration

Usage Guideline Any unmapped VLAN is mapped to the CIST instance.

Examples This example shows how to map a range of VLANs to instance 2:

```
Switch(config)#spanning-tree mst configuration
Switch(config-mst)# instance 2 vlans 1-100
```

This example shows how to map a VLAN to instance 5:

```
Switch(config)#spanning-tree mst configuration
Switch(config-mst)# instance 5 vlans 1100
```

Verify the settings by entering the **show spanning-tree mst configuration** command.

interface

Enter the **interface** command to go into interface configuration mode. The command executed in this mode will be applied to the interface specified by the command.

interface *INTERFACE-ID*

Syntax Description	
INTERFACE-ID	The interface can be a physical port, port-channel, or VLAN.

Default None

Command Mode Global configuration

Usage Guideline The **interface** command puts the command line interface into interface configuration mode for a specified interface.

For the port-channel interface, it must be an existing channel-group.

For the VLAN interface, it must be a previously created VLAN.

Example This example shows how to enter the interface configuration mode for eth2.5:

```
Switch(config)# interface eth2.5
Switch(config-if)#
```

interface range

Enter the **interface range** command to go into interface range configuration mode. The command executed in this mode will be applied to all interfaces specified by the command.

interface range *INTERFACE-ID* **[, | -]**

Syntax Description	
INTERFACE-ID	The interface can be physical port, port-channel, or IP interface.
,	Specifies a series of interface, or separate a range of interfaces from a previous range. No space before and after the comma.
-	Specifies a range of interfaces. No space before and after the hyphen.

Default None

Command Mode Global configuration

Usage Guideline This command puts the command line interface into configuration mode for the specified range of interfaces. The interfaces specified in a range can be different types, such as eth2.1-2.5, vlan100-200.

Example This example shows how to enter the interface configuration mode for a range of ports from eth2.1-2.5.

```
Switch(config)# interface range eth2.1-2.5
Switch(config-if)#
```

interface tunnel

Use the i**nterface tunnel** configuration command to add a tunnel and to enter the interface configuration mode. Use the **no interface tunnel** configuration command to remove a tunnel.

interface tunnel {tunnel-ID}

no interface tunnel {tunnel-ID}

Syntax Description	
tunnel-ID	Specifies the ID of the tunnel to be added, removed or configured. The valid tunnel ID range is 1-127.

Default None

Command Mode Global configuration

Usage Guideline None

Examples The following example will add a tunnel of 2, and then enter into the interface configuration mode.

```
Switch(config)# interface tunnel 2
Switch (config-if)#
```

The following example will remove IPv6 tunnel 2.

```
Switch(config)# no interface tunnel 2
Switch (config)#
```

ip access-group

Use the **ip access-group** command to specify the IP access-list to be applied to an interface. Use the no form of this command to remove an IP access list.

ip access-group *NAME* **[in]**

no ip access-group *NAME* **[in]**

Syntax Description	
NAME	The name of the IP access-list to be applied. Up to 32 characters are allowed. The syntax is a general string that does not allow spaces.
in	(Optional) Specifies that the IP access-list will be applied to ingress traffic. If no option is specified, in direction is applied.

Default None

Command Mode Interface configuration

Usage Guideline One MAC access-list, one IP access-list and one IPv6 access-list can be to the same interface. An error message is displayed if the user attempts to apply the second IP access list.

The IP access list must be created before it can be applied to an interface. An error message is displayed if a list has not yet been created.

The keyword **in** specifies ingress direction check.

The association of an access-group with an interface will consume the filtering entry resources in the switch controller. If the command is applied successfully, the number of remaining entries is displayed. If the access-group contains a rule with a port operator (e.g. gt/lt operator), the number of remaining rules for the port operator is displayed. If the resource is insufficient to commit the command, an error message is displayed.

There is a limitation on the number of port selectors that can be applied.

If the maximum number of available port selectors is exceeded an error message is displayed.

Example This example shows how to specify the IP access-list Strict-Control as an IP access group for eth3.2

```
Switch(config)# interface eth3.2
Switch(config-if)#ip access-group Strict-Control
```

Verify the settings by entering the **show access-group** privileged EXEC command.

ip access-list

Use the command to create or modify an IP access list. This command enters the user interface into the **ip access-list configuration** mode. Use no command to remove an IP access-list.

ip access-list [extended] *NAME*

no ip access-list [extended] *NAME*

Syntax Description	
extended	(Optional) Used to create an IP access list (a list of related IP addresses such as source IP addresses or destination IP adresses) or an IP extended access-list (more information can be chosen).
NAME	The name of the IP access list to be configured. The syntax is a general string that does not allow spaces, up to 32 characters in length.

Default Deny all traffic (implicit).

Command Mode Global configuration

Usage Guideline The access list is always terminated by an implicit deny statement for all traffic and that is the default statement.

When applying an IP access list to an interface, only one IP access list can be applied.

The name must be unique among all (including MAC, IP, or IPv6) access-lists and the characters are case sensitive.

An error message will appear if the allowed number is exceeded after execution of the command.

An IP access list can not be deleted if it is applied at an interface.

An IP extended access-list can only be grouped with an interface, but not any other S/W modules (such as PIM-DM, etc).

Examples This example shows how configure an extended IP access-list, named Strict-Control and an IP access list, named pim-srcfilter.

```
Switch(config)#ip access-list extended Strict-Control
Swtich(config-ip-ext-acl)#permit tcp any 10.20.0.0 255.255.0.0
Swtich(config-ip-ext-acl)#exit
Swtich(config)#ip access-list pim-srcfilter
Switch(config-ip-acl)#permit host 172.16.65.193 any
Switch(config-ip-acl)#
```

Verfiy the settings by entering the **show access-list** command.

ip address

Use **ip address** to set a primary or secondary IP address for an interface, or acquire an IP address on an interface from DHCP. Use the no form of the command to remove the IP settings configuration from the interface.

ip address { *IP-ADDRESS SUBNET-MASK* **[secondary] | dhcp }**

no ip address [*IP-ADDRESS SUBNET-MASK* **]**

Syntax Description	
IP-ADDRESS	The IP address to configure the interface with.
SUBNET-MASK	The mask for the associated IP subnet of the IP address.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.
dhcp	Acquire an IP address on an interface from the DHCP protocol.

Default 0.0.0.0/32.

Command Mode VLAN Interface configuration

Usage Guideline Only VLAN interfaces are valid for this command.

An interface can have one primary IP address and multiple secondary IP addresses. IP processing can be disabled on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, an error message appears on the console.

The optional **secondary** keyword allows assignment of multiple secondary addresses. Secondary addresses are treated like the primary address, except that the system does not generate datagrams other than a routing update packet with secondary source addresses. For example, an SNMP trap is always generated with the primary address. However, the system can respond to a packet sent to the secondary address.

For now, only VLAN interfaces can be configured by this command.

If a VLAN interface has been configured with static IP address (except 0.0.0.0) or DHCP, a Layer 3 IP interface is created.

The **no ip address** command will remove all of the IP settings from the interface.

Example This example (on the next page) shows how to set 10.108.1.27 as the primary address and 192.31.7.17 and 192.31.8.17 as the secondary addresses for VLAN 100:

```
Switch# configure terminal
Switch(config)# interface vlan100
Switch(config-if)# ip address 10.108.1.27 255.255.255.0
Switch(config-if)# ip address 192.31.7.17 255.255.255.0 secondary
Switch(config-if)# ip address 192.31.8.17 255.255.255.0 secondary
Switch(config)# end
```

Verify the settings by entering the **show ip interface** command.

ip address (management port)

Use the command to set the IP address of the Management Port. Use the no form of this command to revert to the default IP address.

ip address *IP-ADDRESS / PREFIX-LENGTH*

no ip address

Syntax Description	
IP-ADDRESS	IP address to be configured for the Management Port.
PREFIX-LENGTH	Prefix Length.

Default 10.90.90.90/8.

Command Mode Management interface configuration

Usage Guideline This is the IP address used for management access to the system. Use **no ip address** command to restore the default IP address 10.90.90.90/8.

Example This example shows how to set 10.1.1.1 as the IP address of the Management Port.

```
Switch#configure terminal
Switch(config)#mgmt-if
Switch(mgmt-if)#ip address 10.1.1.1/8
Switch(mgmt-if)#end
```

Verify the settings by entering the **show mgmt-if** command.

ip address-list

Use this command to specify the IP addresse range in a DHCP address pool and one of which is allowed to be bound with a DHCP client. Use the no form of this command to remove the range of IP addresses from the DHCP address pool.

ip address-list *IP-ADDRESS* **[,|-]**

no ip address-list *IP-ADDRESS* **[,|-]**

Syntax Description	
IP-ADDRESS **[,|-]**	The IP address list to be added into DHCP address pool.

Default No IP addresses exist in any DHCP pool.

Command Mode DHCP pool configuration

Usage Guideline This command is used to define the IP address list for a DHCP pool. Reasonable IP addresses should be carefully defined for the pool. For example, use the same network ID or same subnet for the all IP addresses.

Specify a host by specifying the IP address explicitly or specify a range of IP addresses using a hyphen between the start IP address and end IP address. Both the host and the range of IP addresses can be mixed together. Verify and confirm that the IP addresses chosen are part of the same network.

Example This example shows how to configure the IP address range for pool1 in the IP address range of 10.1.1.1~10.1.1.255 and exclude the address 10.1.1.200 from the pool.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp)# ip address-list 10.1.1.1-10.1.1.255
Switch(config-dhcp)# no ip address-list 10.1.1.200
Switch(config-dhcp)#
```

Verify the address pool is added with the **show ip dhcp pool** command.

ip dhcp screening ports

Use the command to configure the state of the function for filtering of DHCP server packet on ports and Use the no form of this command to disable function on ports.

ip dhcp screening ports *INTERFACE-ID* **[, | -]**

no ip dhcp screening ports *INTERFACE-ID* **[, | -]**

Syntax Description	
INTERFACE-ID	The interface should be a physical port or port channel.
,	Specify a series of interface, or spearate a range of interfaces from a previous range. No space before and after the comma.
-	Specify a range of interfaces. No space bfore and after the hyphen.

Default Not configured

Command Mode Global configuration mode

Usage Guideline Use this command to enable per port control of the DHCP server screening function. If a port is configured to enable DHCP server screening function, it will deny all DHCP server packets (UDP source port = 67). You can add a permit binding rule by command "**ip dhcp screening**".

Example The following example enable the DHCP server screening function on port eth4.1 and eth5.3:

```
switch# configure terminal
switch(config)#ip dhcp screening ports eth4.1,eth5.3
```

ip dhcp screening

Use this command to add/delete the DHCP server/client binding entry.

ip dhcp screening server-ip *IP-ADDRESS* **[client-mac** *MAC-ADDRESS***] ports** *INTERFACE-ID* **[, | -]**

no ip dhcp screening server-ip *IP-ADDRESS* **[client-mac** *MAC-ADDRESS***] ports** *INTERFACE-ID* **[, | -]**

Syntax Description	
IP-ADDRESS	DHCP server IP address.
client-mac *MAC-ADDRESS*	(Optional) Client MAC address to be associated with a server IP address. It represents “All Client MAC” if not specified.
INTERFACE-ID **[,	-]**	The interface should be a physical port or port channel which will be applied. Specify a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma. Specifies a range of interfaces. No space before and after the hyphen.

Default Not configured

Command Mode Global configuration mode

Usage Guideline This command is used to specify explicit "permit" rules for the 3-tuple (DHCP server IP, client's MAC, port list from which DHCP server is allowed come) to allow DHCP server packets. DHCP server packets except those met explicated configured met the server IP /.client MAC binding will be filtered on specified ports. If client MAC address is not specified, then DHCP server packets will pass as long as .the server IP matches.

Note: The user needs turn on the port's "DHCP Server Screening" to make all DHCP server packets are denied by default by command: "**ip dhcp screening ports**". If a port's "DHCP Server Screening" doesn't turn on, the "permit" rule is not effective

Example The following example configures a permit rule to allow DHCP server packet with souce IP address 10.1.1.1 and client MAC address 00-08-01-02-03-04 on eth4.1-4.34

```
switch#configure terminal
switch(config)#ip dhcp screening server-ip 10.1.1.1 client-mac 00-08-01-02-03-04 ports eth4.1-4.34
```

ip dhcp screening trap-log

Used to enable trap/log function and use the no form to disable trap/log function.

ip dhcp screening trap-log

no ip dhcp screening trap-log

Syntax None

Default Disabled

Command Mode Global configuration mode

Usage Guideline Use this command to enable the function of trap/log. It will log illegal server IP address, ingress port and send trap if any DHCP server packet is not authorized and dropped if user turns on this function.

Example The following example shows to enable trap/log function of DHCP screening:

```
switch#configure terminal
switch(config)# ip dhcp screening trap-log
```

ip dhcp snooping

Use this command to globally enable DHCP snooping. Use no command to disable DHCP snooping.

ip dhcp snooping

no ip dhcp snooping

Syntax None

Default Disabled

Command Mode Global configuration

Usage Guideline The DHCP snooping function snoops the DHCP packets arriving at the un-trusted interface on VLAN that is enabled for DHCP snooping. With this function, the DHCP packets coming from the un-trusted interface can be validated, and a DHCP binding database will be constructed for the DHCP snooping enabled VLAN. The binding database provides IP and MAC binding information that can be further used by the IP source guard and dynamic ARP inspection process.

Use the ip dhcp snooping command to globally enable DHCP snooping. Use the ip dhcp snooping vlan command to enable DHCP snooping for a VLAN. DHCP snooping process occurs during the relay agent relays the packet. To enable the DHCP relay service, relay agent service must be enabled by service dhcp command, and the server address to relay the packet must be configured by the ip dhcp relay address.

Example These examples shows how to enable and disable DHCP snooping:

```
Switch# configure terminal
Switch(config)# ip dhcp snooping
Switch(config)#

-----------------------------------------

Switch# configure terminal
Switch(config)# no ip dhcp snooping
Switch(config)#
```

ip dhcp snooping information option

Use this command to globally allow DHCP packets with relay option 82 on the un-trusted interface. Use the no form of the command to not allow the packets with relay option 82.

ip dhcp snooping information option allow-untrusted

no ip dhcp snooping information option allow-untrusted

Syntax None

Default Not allow

Command Mode Global configuration

Usage Guideline The DHCP snooping function validates the DHCP packets when it arrives at the port on the VLAN that is enabled for DHCP snooping. By default, the validation process will drop the packet If gateway addr !=0 or option 82 is present.

Use the ip dhcp snooping information option allow-untrusted command to allow the packet with relay option 82 arriving at the un-trusted interface.

.

Example This example shows how to enable DHCP snooping option-82 allow untrusted port:

```
Switch# configure terminal
Switch(config)# ip dhcp snooping information option allow-untrusted
Switch(config)#
```

This example shows how to disable DHCP snooping option-82 allow untrusted port:

.

```
Switch# configure terminal
Switch(config)# no ip dhcp snooping information option allow-untrusted
Switch(config)#
```

ip dhcp snooping trust

Use this command to configure a port as interface trusted for DHCP snooping. Use the no form of this command to return to the default setting.

ip dhcp snooping trust

no ip dhcp snooping trust

Default Disabled

Command Mode Interface configuration

Usage Guideline The command is available for physical port configuration.

Normally, the ports connected to DHCP server or to other switches should be configured as a trusted interface. The ports connected to DHCP clients should be configured as un-trusted interface.

When a port is configured as an un-trusted interface, the DHCP message arrives at the port on a vlan that is enabled for DHCP and snooping will be validated by the following checks.

(1)The received message should be all sent by the client. If the message is sent by the DHCP server, the message will be dropped.

(2)If ip dhcp snooping verify mac-address is enabled, the source MAC in the Ethernet header must be the same as the DHCP client hardware address to pass the validation.

(3)For the received release and decline packets, the received port is also checked against the binging database entry. The packet will be dropped if inconsistent.

(4)If gateway addr !=0 or option 82 is present, the packet is dropped

In addition to doing the validation, DHCP snooping also create a binding entry based on the IP address assigned to client by the server in DHCP snooping binding database. The binding entry contains information including MAC address, IP address, the VLAN ID and port ID where the client is located, and the expiry of the lease time.

Example This example shows how to enable DHCP snooping trust for port 3.3:

```
Switch(config)# interface eth3.3
Switch(config-if)# ip dhcp snooping trust
Switch(config)#
```

ip dhcp screening suppress-duration

Used to set the suppressed duration for trap/log and use the **no** form of this command to restore back to default setting.

ip dhcp screening suppress-duration *SUPPRESS-TIME*

no ip dhcp screening suppress-duration

Syntax Description	
SUPPRESS-TIME	The monitoring interval The valid value is between 1 and 30. Default value: 10 minutes Until: minute.

Default 10 minutes

Command Mode Global configuration mode

Usage Guideline Use this command to set the interval that device will send trap when illegal DHCP server is detected. The same illegal DHCP server IP address detected just is send once to the trap receivers within the specified ceasing unauthorized duration.

Example The following example shows to specify the suppress time to 20 minutes:

```
switch#configure terminal
switch(config)# ip dhcp screening suppress-duration 20
```

ip arp inspection trust

Use the command to trust an interface for dynamic ARP inspection. Use the no form of the command to disable the trust state.

ip arp inspection trust

no ip arp inspection trust

Syntax Description Not applicable.

Default un-trusted

Command Mode Interface configuration mode

Usage Guideline The command is available for physical port configuration.

When an interface is in ip arp inspection trust state, the ARP packets arriving at the interface will not be inspected. When an interface is in ip arp inspection untrust state, the ARP packets arriving at the port and belong to the VLAN that is enabled for inspection will be inspected.

Example This example shows how to configure port 3.3 to be trusted for DAI:

```
Switch# configure terminal
Switch(config)# interface eth3.3
Switch(config-if)# ip arp inspection trust
Switch(config-if)#
```

ip arp inspection validate

Use the command to specify the additional checks to be performed during ARP inspection check. Use the **no** form of the command to remove specific additional check.

ip arp inspection validate {[src-mac] [dst-mac] [ip]}

no ip arp inspection validate [src-mac] [dst-mac] [ip]

Syntax Description	
src-mac	(Optional) Specify to check, for both ARP request response packets, the consistency of the source MAC address in the Ethernet header against the sender MAC address in the ARP payload.
dst-mac	(Optional) Specify to check, for ARP response packets, the consistency of the destination MAC address in the Ethernet header against the target MAC address in the ARP payload.
ip	(Optional) Checks the ARP body for invalid and unexpected IP addresses. Specify to check the validity of IP address in the ARP payload. Sender IP in both ARP request and response and target IP in ARP response are validated. Packets with addresses including 0.0.0.0, 255.255.255.255, and all IP multicast addresses are dropped. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

Default Disabled

Command Mode Global configuration mode

Usage Guideline Use the command to specify the additional checks to be performed during dynamic ARP inspection check. The specified check will be performed on packets arriving at the untrusted interface and belong to the VLANs that are enabled for ip arp inspection.

Use the no form of the command with specific option to disabled specific type of check.

Example This example shows how to enable source MAC validation:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate src-mac
Switch(config)#
```

This example shows how to disable source MAC validation:

```
Switch# configure terminal
Switch(config)# no ip arp inspection validate src-mac
Switch(config)#
```

ip arp inspection vlan

Use the command to enable specific VLANs for dynamic ARP inspection. Use the **no** form of the command disable dynamic ARP inspection for VLAN.

ip arp inspection vlan *VLAN-ID* [, | -]

no ip arp inspection vlan *VLAN-ID* [, | -]

Syntax Description	
vlan *VLAN-ID*	Specify the VLAN to enable or disable the ARP inspection function.
,	(Optional) Specify a series of VLANs, or separate a range of VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specify a range of VLANs. Enter a space before and after the hyphen.

Default ARP inspection is disabled on all VLANs.

Command Mode Global configuration mode

Usage Guideline When a VLAN is enabled for ARP inspection, the ARP packets, including both ARP request and response packet belonging to the VLAN arriving at the un-trusted interface will be validated. If the IP to MAC address binding pair the source MAC address and the source IP address in the Ethernet header is not permitted by the ARP ACL or the DHCP snooping binding database, the ARP packet will be dropped.

Example This example shows how to enable ARP inspection on VLAN2:

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 2
Switch(config)#
```

ip verify source vlan dhcp-snooping

Use this command to enable IP source guard for a port. Use the no form of the command to disable IP source guard.

ip verify source vlan dhcp-snooping port-security

no ip verify source vlan dhcp-snooping port-security

Syntax Description	
port-security	Specify to check both IP address and MAC address of the recieved IP packets.

Default Disabled

Command Mode Interface configuration mode

Usage Guideline The command is available for physical port configuration.

Use the command the enable the IP source guard on the configured port.

When a port is enabled for IP source guard, the IP packet arrives at the port will be validated via port ACL. Port ACL is a hardware mechanism and its entry can come from either the manual configured entry or the DHCP snooping binding database. The packet fails to pass the validation will be dropped.

The validation is based on both the source MAC address and IP address. The IP to MAC address binding pair must match the entries in port ACL to pass the validation.

Example This example shows how to enable IP Source Guard for port 3.1:

```
Switch# configure terminal
Switch(config)# interface eth3.1
Switch(config-if)# ip verify source vlan dhcp-snooping port-security
Switch(config-if)#
```

ip source binding

Use this command to create a static entry used for IP source guard. Use the no form of the command to delete a static entry.

ip source binding *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *PORT* **[**, | -]

no ip source binding *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *PORT* [, | -]

Syntax Description

MAC-ADDRESS	Specifies the MAC address of the IP to MAC address binding entry.
vlan *VLAN-ID*	Specified the VLAN that the valid host belongs to.
IP-ADDRESS	Specifies the IP address of the IP to MAC address binding entry.
PORT	Specified the port that the valid host is connected.
,	(Optional) Specify a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specify a range of interfaces. No space before and after the hyphen.

Default No entry is configured

Command Mode Global configuration mode

Usage Guideline Use the command to create a static binding entry used for IP source guard check.

Use the no command to delete a static binding entry. The parameters specified for the command must exact match the configured parameter to be deleted.

If the MAC address and the VLAN for the configured entry already exist, the existing binding entry is updated.

The interface specified for the command can be a physical port interface.

Example This example shows how to configure an IP Source Guard entry with IP address 10.1.1.1 and MAC address 00-01-02-03-04-05, at VLAN 2 on interface eth3.10:

```
Switch# configure terminal
Switch(config)# ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1
interface eth3.10
Switch#
```

This example shows how to delete an IP Source Guard entry with IP address 10.1.1.1 and MAC address 00-01-02-03-04-05, at VLAN 2 on interface eth3.10:

```
Switch# configure terminal
Switch(config)# no ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1
interface eth3.10
Switch#
```

ip as-path access-list

Use this command to define a BGP Autonomous System (AS) path access list. Use the **no** form of this command to disable use of the access list.

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

no ip as-path access-list *ACCESS-LIST-NAME*

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

Default None

Command Mode Global configuration

Usage Guideline The named community access list is a filter based on regular expressions. If the regular expression matches the specified string representing the AS path of the route, then the **permit** or **deny** condition applies. Use this command to define the BGP access list globally, use the neighbor filter-list command in the router configuration mode to apply a specific access list.

Multiple commands can be applied to a list name.

Example This example shows how to define an AS path access list named “mylist” to deny access to the neighbor with AS number 65535:

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

Verify the settings by entering the **show ip as-path access-list** command.

ip community-list

Use this command to add a community list entry. Use the **no** form of this command to delete the community list entry.

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

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

Syntax Description	
COMMUNITY-LIST-NAME	Specifies the community list name. The syntax is a general string up to 32 characters in length with no spaces.
permit	Specifies the community to accept.
deny	Specifies the community to reject.
COMMUNITY	This is a user-specified number (32-bits integer) 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. **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.

Default BGP community exchange is not enabled 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

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.

This command can be applied multiple times.

In the command **no ip community access-list** *COMMUNITY-LIST-NAME* if a permit or deny keyword is not specified, then all community lists bonded at the specified access list will be removed.

Example This example (on the next page) shows how to configure a community list

named“mycommlist” that permit routes from network 10 in autonomous system 50000:

```
Switch(config)# ip community-list mycommlist permit 50000:10
```

Verify the settings by entering the **show ip community-list** command.

ip dhcp snooping verify MAC-address

Use this command to enable the verification that the source MAC address in a DHCP packet matches the client hardware address. Use the no command to disable the verification of the MAC address.

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Syntax None

Default Disabled

Command Mode Global configuration

Usage Guideline The DHCP snooping function validates the DHCP packets when it arrives at the port on the VLAN that is enabled for DHCP snooping.

By default, DHCP snooping will verify that the source MAC in the Ethernet header be the same as the DHCP client hardware address to pass the validation.

Use the no ip dhcp snooping verify mac-address to disable the check for the MAC address.

Example This example shows how to enable the verification that the source MAC address in a DHCP packet matches the client hardware address

```
Switch# configure terminal
Switch(config)# ip dhcp snooping verify mac-address
```

ip dhcp snooping vlan

Use this command to enable DHCP snooping on a VLAN or a group of VLANs. Use no command to disable DHCP snooping on a VLAN or a group of VLANs.

ip dhcp snooping vlan *VLAN-ID* **[, | -]**

no ip dhcp snooping vlan *VLAN-ID* **[, | -]**

Syntax Description	
vlan *VLAN-ID*	Specify the VLAN to enable or disable the DHCP snooping function.
,	(Optional) Specify a series of VLAN's, or separate a range of VLAN's from a previous range. Enter a space before and after the comma.
-	(Optional) Specify a range of VLANs. Enter a pace before and after the hyphen.

Default None

Command Mode Global configuration mode

Usage Guideline Use the ip dhcp snooping command to globally enable DHCP snooping and use the ip dhcp snooping vlan command to enable DHCP snooping for a VLAN. DHCP snooping process occurs during the relay agent relaying the packet.

The DHCP snooping function snoops the DHCP packets arriving at the un-trusted interface on VLAN that is enabled for DHCP snooping. With this function, the DHCP packets that come from an un-trusted interface can be validated, and a DHCP binding database will be constructed for the DHCP snooping enabled VLAN. The binding database provides IP and MAC binding information that can be further used by the IP source guard and dynamic ARP inspection process.

The DHCP snooping enabled status for a secondary VLAN follows the status for its primary VLAN. Thus, the DHCP snooping setting does not take effect if it is configured on a secondary VLAN.

Example This example shows how to enable DHCP snooping on vlan10:

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 10
Switch(config)#
```

This example shows how to disable DHCP snooping on vlan10:

```
Switch# configure terminal
Switch(config)# no ip dhcp snooping vlan 10
Switch(config)#
```

This example shows how to enable DHCP snooping on range of VLAN:

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 10,15-18
Switch(config)#
```

This example shows how to disable DHCP snooping on range of VLAN:

```
Switch# configure terminal
Switch(config)# no ip dhcp snooping vlan 10,15-18
Switch(config)#
```

ip dhcp ping packets

User this command to specify the number of packets that the DHCP server will send as a part of the ping operation. Use the no form of this command to prevent the server from pinging pool addresses.

ip dhcp ping packets *COUNT*

no ip dhcp ping packets

Syntax Description	
COUNT	The number of ping packets the DHCP server will send. From 0 to 10 where 0 stops the ping checks from being sent upon address assignment.

Default Two packets.

Command Mode Global configuration

Usage Guideline Before a DHCP server attempts to assign a pool address a to client, it tries to ping the specific pool address. If the ping packet is unanswered, the DHCP server assumes this pool address is currently available and is safe to assign to a requesting client.

Example The following is a sample of configuring the number of ping packets as 3.

```
switch# configure terminal
switch(config)# ip dhcp ping packets 3
```

ip dhcp ping timeout

Use this command to specify how long the DHCP server will wait for the ping reply from a pool address. Use the no form of this command to restore the wait time for the ping reply back to the default value (500ms).

ip dhcp ping timeout *MILLISECONDS*

no ip dhcp ping timeout

Syntax Description	
MILLISECONDS	The interval of time from 100 to 1000 milliseconds that the DHCP server will wait for a ping reply.

Default 500 milliseconds.

Command Mode Global configuration

Usage Guideline Before the DHCP server attempts to assign a pool address to a client, it tries to ping the specific pool address. If the ping packet is unanswered, the DHCP server assumes this pool address is currently available and is safe to assign to the requesting client. This command sets the time that the DHCP server will wait for a reply from the address that it pinged.

Example The following is sample of configuring the ping timeout as 100.

```
switch# configure terminal
switch(config)# ip dhcp ping timeout 100
```

ip dhcp pool

Use this command to configure a DHCP address pool on a DHCP Server and enter the DHCP pool configuration mode. Use the no form of this command to remove the address pool.

ip dhcp pool *NAME*

no ip dhcp pool *NAME*

Syntax Description	
NAME	The address pool name can either be a symbolic string or an integer. The maximum length is up to 64 charaters.

Default Not configured

Command Mode Global configuration

Usage Guideline This command changes the configuration mode to DHCP pool configuration mode, identified by the (config-dhcp)# prompt. In this mode, the administrator can configure pool parameters, for example, the IP subnet number and default router list.

Note that the DHCP pool name can play an important role if the DHCP host requests meet the IP address offering criteria of more than one DHCP pool. The pool name with the shortest name and lowest alphabet is the only pool allowed to offer the correct IP address to the host.

Example The following example configures the address pool named "pool1".

```
switch# configure terminal
switch(config)# ip dhcp pool pool1
```

ip dhcp relay

Use this command to enable Dynamic Host Configuration Protocol (DHCP) relay agent features on the switch. Use the no form of this command to disable DHCP relay agent features.

ip dhcp relay

no ip dhcp relay

Syntax None

Default Disabled

Command Mode Global configuration

Usage Guideline Use this command to enable DHCP relay function. The DHCP relay function is disabled by default.

Example Enable DHCP relay function:

```
Switch > enable
Switch# configure terminal
Switch(config)# ip dhcp relay
```

Verify the settings by entering the **show ip dhcp relay** command.

ip dhcp relay address

Use this command to specify the DHCP relay server IP address. Use the no form of the command to delete a DHCP server. When using the no form of the command if no IP address is specified, all DHCP servers will be deleted.

ip dhcp relay address *IP-ADDRESS*

no ip dhcp relay address [*IP-ADDRESS* **]**

Syntax Description	
IP-ADDRESS	DHCP server IP address

Default None

Command Mode VLAN Interface configuration

Usage Guideline Use this command to specify the DHCP server IP address. The DHCP request packets received by the device will be relayed to the specified DHCP servers.

Only VLAN interfaces are valid interfaces for this command.

Multiple DHCP server addresses can be specified on the same IP interface.

The specified DHCP servers are only effective when the interface is an IP interface.

For layer 2 devices, the DHCP servers need to be specified on the system IP interface. All the DHCP request packets received by a device will be relayed to these DHCP servers.

For layer 3 devices, all the DHCP request packets received by the IP interfaces will be relayed to the DHCP servers configured on this interface. If there are no DHCP servers configured on an IP interface, then the DHCP request packets will not be relayed. DHCP request packets received by the non-IP interfaces, will be relayed to the first IP interface that has DHCP servers configured.

Example Enable DHCP relay function and set interface VLAN 100 with DHCP server ip address 10.1.1.1, the DHCP packet received on VLAN 100 will relay to DHCP server 10.1.1.1:

```
Switch# configure terminal
Switch(config)# interface vlan100
Switch(config-if)# ip dhcp relay address 10.1.1.1
```

Verify the settings by entering the **show ip dhcp relay** command.

ip dhcp relay hops

Use this command to configure the maximum number of relay hops that the DHCP packets can traverse.

ip dhcp relay hops *HOP-COUNT*

Syntax Description	
HOP-COUNT	The number of relay hops that the DHCP packets can traverse. The valid setting is 1-16. Every time that a DHCP packet is relayed, the relay hop-count will be increment by 1. If the relay hop count in the received packet is equal to or greater then the specified value, the packet will be discarded.

Default 4

Command Mode Global configuration

Usage Guideline Use this command to specify the maximum number of relay hops that the DHCP packets can traverse.

Example This example shows how to set maximum number of router relay hops 5:

```
Switch# configure terminal
Switch(config)#ip dhcp relay hops 5
```

Verify the settings by entering the **show ip dhcp relay** command.

ip dhcp relay information check

Use this command to configure the DHCP relay agent to validate the relay agent information option in the received DHCP reply packet.

ip dhcp relay information check

no ip dhcp relay information check

Syntax None

Default Enabled

Command Mode Global configuration

Usage Guideline When this check for the reply packet is enabled, the device will check that the option-82 field in DHCP reply packets it receives from the DHCP server is valid. If an invalid message is received, the relay agent drops it. If a valid message is received, the relay agent removes the option-82 field and forwards the packet.

If the check is disabled, a packet with an invalid option-82 field will be directly forwarded.

Example Enabled DHCP relay agent check for the reply packet.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information check
```

Verify the settings by entering the **show ip dhcp relay** command.

ip dhcp relay information option

Use this command to enable the insertion of the relay agent information option (option 82). Use the no form of the command to disable this function.

ip dhcp relay information option

no ip dhcp relay information option

Syntax None

Default Disabled

Command Mode Global configuration

Usage Guideline Use this command to enable insertion of DHCP option 82.

When the DHCP 82 option is enabled, a DHCP packet received from a client will have the option 82 field inserted before being relayed to the server. The DHCP option 82 contains 2 suboptions: circuit ID and remote ID sub-options.

If the switch is standalone then the module field, within the circuit ID suboption, is always set to zero. The following describes the format of the Circuit and Remote ID suboption formats:

Circuit ID suboption format:

Byte	1	2	3	4	5	6	7	8
Field	Sub-option Type	Length	Circuit IDType	Length	VLAN ID		Module #	Port #
Value	1	6	0	4	X		X	X

VLAN ID - The incoming VLAN ID of DHCP client packet.

Module # - For a standalone switch, Module # is always 0; For a stackable switch, Module is Unit ID.

Port # - The receiving port number of DHCP client packet, port number starts from 1.

Remote ID suboption format:

Byte	1	2	3	4	5	6	7	8	9	10
Field	Sub-option Type	Length	Remote ID Type	Length	MAC Address					
Value	2	8	0	6	M1	M2	M3	M4	M5	M6

MAC address: the switch's system MAC address.

Example This example shows how to enable insertion of the option-82 field during the relay of DHCP request packets.

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

Verify the settings by entering the **show ip dhcp relay** command.

ip dhcp relay information policy

Use this command to configure the information re-forwarding policy for the DHCP relay agent.

ip dhcp relay information policy {drop | keep | replace}

Syntax Description	
drop	Discards the packet that already has the relay option. This packet represents a packet that is relayed by a relay agent and already has the option inserted.
keep	When the DHCP request packets already have the relay option, then the relay option is left unchanged and directly relayed to the DHCP server.
replace	When the DHCP request packets already have the relay option, then it will be replaced by a new option.

Default **replace**

Command Mode Global configuration

Usage Guideline The device may receive a DHCP request packet that already has the relay option. This packet represents a packet that is relayed by a relay agent and already has the option inserted. The gateway address in the received DHCP packet should not be zero since it represents the IP address of the predecessor DHCP relay agent.

Example This example shows how to set the policy to drop the DHCP request packet that is relayed by other DHCP relay agent and already has option-82 inserted.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information policy drop
```

Verify the settings by entering the **show ip dhcp relay** command.

ip dhcp relay information trust-all

Use this global command to direct the DHCP relay agent to accept the packets with giaddr==0 (this relay agent is the first relay of this DHCP request packet) and the relay agent information option already present in the packet. Use the no form of the command to specify to drop these DHCP request packets.

ip dhcp relay information trust-all

no ip dhcp relay information trust-all

Syntax None

Default The interface default is un-trusted.

Command Mode Global configuration

Usage Guideline When the IP DHCP relay information is trusted, and the gateway address in the DHCP request packet is set to all zeros, but the relay agent information option is present in the packet, then the DHCP relay agent will accept the packet.

When the packet is not trusted, then it will be discarded.

This command is under global configuration; it will enable/disable all existing VLANs' DHCP Relay Agent trusted relay agent information. However, the command takes effect only in the running configuration and is not kept in NVRAM for the next boot cycle using the startup configuration.

To configure a specific interface's trust status, use the **ip dhcp relay information trusted** interface command.

Example This command shows how to enable all interfaces with the DHCP relay agent set to accept the packets with giaddr==0 and the relay agent information option already present in the packet.

```
Switch# configure
Switch(config)# ip dhcp relay information trust-all
Swtich(config)#
```

Verify the settings by entering the **show ip dhcp relay information trusted-sources** command

ip dhcp relay information trusted

Use this interface command to direct the DHCP relay agent to accept the packets with giaddr==0 (this relay agent is the first relay of this DHCP request packet) and relay agent information option is already present in the packet. Use the no form of the command to configure to drop these DHCP request packet.

ip dhcp relay information trusted

no ip dhcp relay information trusted

Syntax None

Default The interface default is un-trusted.

Command Mode VLAN interface configuration

Usage Guideline When IP DHCP relay information is trusted, if the gateway address in the DHCP request packet is set to all zeros but the relay agent information option is already present in the packet, the DHCP relay agent will accept the packet.

If it is un-trusted, then the packet will be discarded.

Example This example shows how to enabled interface vlan100's DHCP relay agent to accept the packets with giaddr==0 and relay agent information option is already present in the packet.

```
Switch# configure
Switch# interface vlan100
Switch(config-if)# ip dhcp relay information trusted
Swtich(config-if)# end
```

Verify the settings by entering the **show ip dhcp relay information trusted-sources** command.

ip dvmrp

Use this command to enable DVMRP on the current interface. Use the no form to disable DVMRP on the interface.

ip dvmrp

no ip dvmrp

Syntax None

Default Disabled

Command Mode VLAN interface configuration

Usage Guideline This command is only valid for the VLAN interface.

The VLAN interface will have DVMRP protocol enabled (or disabled).

Before enabling DVMRP function on an interface, it is necessary to enable IP multicast routing with the **ip multicast-routing** command in global configuration mode.

Only one multicast routing protocol can be enabled on an interface, make sure no other multicast routing protocol is configured before DVMRP is enabled . If another protocol is enabled, an error messge is displayed.

Example This example shows how to enable the DVMRP protocol on the interface VLAN 1.

```
Switch(config)# interface vlan1
Switch(config-if)# ip dvmrp
```

Verify the settings by the **show ip dvmrp interface** command.

ip dvmrp metric

Use this command to configure the metric value on the current interface.

ip dvmrp metric *METRIC*

Syntax Description	
METRIC	It can be a value from 1 to 31. A value of 32 sets the route metric to infinite or unreachable.

Default 1

Command Mode VLAN interface configuration

Usage Guideline This command is only valid for the VLAN interface.

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. DVMRP uses the infinite or unreachable metric which is defined to be 32. This limits the breadth across the entire DVMRP network and is necessary to place an upper boundary on the convergence time of the protocol.

By default, a metric value of 1 is associated with each DVMRP route. Use the command to modify the metric value.

Example This example shows how to change the metric value to 2 of an interface.

```
Switch(config)# interface vlan1
Switch(config-if)# ip dvmrp metric 2
```

Verfiy the settings by the **show ip dvmrp interface** command.

ip http server

Use this command to enable HTTP server. Use the no form of the command to disable HTTP server function.

ip http server

no ip http server

Syntax None

Default HTTP interface is enabled.

Command Mode Global configuration

Usage Guideline This command enables HTTP server function.

Example This example will disable the http server

```
Switch(config)# no ip http server
```

Verify the settings by entering the **show system protocol-state** command.

ip http service-port

Use this command to specify the HTTP service port. And use the default command to return the service port to 80.

ip http service-port *TCP-PORT*

default ip http service-port

Syntax Description	
TCP-PORT	TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the HTTP protocol is 80.

Default Port 80

Command Mode Global configuration

Usage Guideline This command configures the TCP port number for HTTP.

Example This example set HTTP TCP port number to 100

```
Switch(config)# ip http service-port 100
```

Verify the settings by entering the **show system protocol-state** command.

ip igmp access-group

Using the **ip igmp access-group** command in interface configuration restricts a subnet's hosts to join only multicast groups that are permitted by an IP basic access list. It also can be used to restrict hosts (receivers) on a subnet to membership of only the (S,G) channels that are permitted by an IP basic access list. To disable the restrictions, use the no form of this command.

ip igmp access-group *IP-ACL*

no ip igmp access-group

Syntax Description	
IP-ACL	Specifies an IP basic access list. (not an IP extended access list). There are two types of IP ACL lists. One is the IP basic ACL list used to consider only the packet IP address. The other list is the IP extended ACL which uses the packet's IP address as well as other IP information such as UDP/TCP port number, TOS, etc..

Default No access group is set.

Command Mode VLAN interface configuration

Usage Guideline Use the ip igmp access-group command to filter groups from IGMP reports by using an IP basic access list. It also can filter sources and groups from IGMPv3 reports by using an IP basic access list. This command is used to restrict hosts on a subnet to join only multicast groups that are permitted by an IP basic access list. The command can also restrict hosts on a subnet to membership of only those (S, G) channels that are permitted by an IP basic access list.

An IGMP access list accepts only an IP basic access list, allowing membership reports to be filtered based only on multicast group addresses.

IGMPv3 allows multicast receivers not only to join to groups, but to groups based on including or excluding sources. For appropriate access control, it is therefore necessary to allow filtering of IGMPv3 messages not only by group addresses reported, but by group and source addresses.

Example This example shows how to restrict the serviced IGMP group for VLAN 1000 to group 226.1.1.1. In the following example, at first, create an IP basic access list named igmp_filter which only permits the packets with destination is group address 226.1.1.1. Then, associate this access group in interface VLAN 1000.

```
Switch#configure terminal
Switch(config)# ip access-list igmp_filter
Switch(config-ip-acl)#permit any 226.1.1.1 255.255.255.255
Switch(config-ip-acl)# exit
Switch(config)# interface vlan1000
Switch(config-if)# ip igmp access-group igmp_filter
Switch(config-if)# end
```

Verfiy the settings by entering the **show ip igmp interface** command.

ip igmp last-member-query-interval

Use this command to configure the interval at which the router sends IGMP group-specific or group-source-specific (with IGMP Version 3) query messages. The command sets the timer value for both IGMP L3 queries and IGMP snooping.

ip igmp last-member-query-interval *MILLISECONDS*

Syntax Description	
MILLISECONDS	Interval, in milliseconds, at which IGMP group-specific or group-source-specific (with IGMP Version 3) query messages are sent. The range is 1000 to 25000.

Default 1000 milliseconds

Command Mode VLAN interface configuration

Usage Guideline When an IGMP querier receives a leave packet, it will send a group specific query or group source specific query. The leave timer starts once the IGMP querier receives a leave packet from an interface. If the interface does not receive the report packet before the leave timer expires, then the interface's membership will be removed from the group or channel that is to be leaved. The value of the leave timer is the value of the *last-member-query-interval* * the *last-member-query-count*.

The IGMP last-member-query-interval will be carried within IGMP group-specific queries or group-source-specific (with IGMP Version 3) query messages.

The *last-member-query-count* will have the same value as the *robustness-variable*.

When IGMP is disabled but IGMP snooping is enabled at the interface, then the IGMP *last-member-query-interva*l value set with this command is used for IGMP snooping. If the command **"ip igmp snooping immediate-leave" on page 266** is enabled, then this timer value is ignored and the interface's group or channel membership, identified in the leave request from the host, will be immediately removed from the IGMP snooping membership table.

Example This example shows how to configure IGMP last member query interval value. It configures IGMP last member query interval value to 2 seconds on interface VLAN 1000.

```
Switch#configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ip igmp last-member-query-interval 2000
Switch(config-if)# end
```

Verify the settings by entering the **show ip igmp interface** command.

ip igmp query-interval

Use this command to configure the interval at which the router sends IGMP general-query messages periodically.

ip igmp query-interval *SECONDS*

Syntax Description	
SECONDS	Configure the frequency at which the designated router sends IGMP general-query messages. By default, the designated router sends IGMP general-query messages every 125 seconds to keep the IGMP overhead very low on the hosts and networks. The range is 1 to 31744.

Default 125 seconds

Command Mode VLAN interface configuration

Usage Guideline This command is for use on the VLAN interface only. Use this Interface configuration command for modifying IGMP Group Member Query Interval on an interface.

The IGMP querier sends IGMP membership query messages at the interval specified by the **ip igmp query-interval** command to discover which multicast groups have members on the attached networks of the router. Hosts respond with IGMP report messages indicating that they want to receive multicast packets for specific groups (that is, indicating that the host wants to become a member of the group). IGMP query messages are addressed to the all-hosts multicast group, which has the address 224.0.0.1, and has an IP time-to-live (TTL) value of 1.

The igmp query-interval is also used for igmp snooping as IGMP is disabled but igmp snooping is enabled at the interface.

Example This example shows how to configure the IGMP query interval to 300 seconds on interface VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ip igmp query-interval 300
Switch(config-if)# end
```

Verify the settings by entering the **show ip igmp interface** command.

ip igmp query-max-response-time

Use this command to configure the maximum response time advertised in IGMP queries.

ip igmp query-max-response-time *SECONDS*

Syntax Description	
SECONDS	Set the maximum response time, in seconds, advertised in IGMP queries.The range is 1 to 25.

Default 10 seconds

Command Mode VLAN interface configuration

Usage Guideline This command controls the period during which the group member can respond to an IGMP query message before the router deletes the membership.

This command applies to interfaces configured for both IGMP Layer-3 multicast protocols and IGMP Snooping (L2 mode and the interface function as a querier). The group membership interval is equal to query-interval* robustness + max response time.

Example This example shows how to configure IGMP max query response time to 10 seconds on VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ip igmp query-max-response-time 10
Switch(config-if)# end
```

Verify the settings by entering the **show ip igmp interface** command.

ip igmp robustness-variable

Use this command to tune for the expected packet loss on a network, i.e. the Robustness Variable of IGMP.

ip igmp robustness-variable *VALUE*

Syntax Description

VALUE	Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals: • Group membership interval - Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable * query interval) + (1 * query response interval). • Other querier present interval - Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable * query interval) + (0.5 * query response interval). • Last member query count - Number of group-specific queries or group-source-specific (with IGMP Version 3) query messages sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable. The robustness variable range is from 1 to 7.

Default *VALUE*: 2

Command Mode VLAN Interface configuration

Usage Guideline This command is valid for the VLAN interface only. Use this command to modify the IGMP Robustness Variable on an interface.

The IGMP Robustness Variable determines the number of general queries that IGMP sends before aging out a multicast address when there is no IGMP report response. In other words, this variable is also used as "last member query count". The group membership interval is equal to query-interval* robustness + max response time.

The larger the Robustness Variable is set, the higher IGMP protocol packet loss is acceptable. IGMP can recover from robustness variable minus 1 lost IGMP packet.

Example This example shows how to configure IGMP Robustness Variable value. It configures IGMP Robustness Variable value to 5 on interface VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ip igmp robustness-variable 5
Switch(config-if)# end
```

Verify the settings by entering the **show ip igmp interface** command.

ip igmp snooping

Use this command to enable IGMP Snooping function on the switch. Use the no form of this command to disable IGMP Snooping function.

ip igmp snooping

no ip igmp snooping

Syntax None

Default IGMP snooping is disabled on all VLAN interfaces

The IGMP snooping global state is disabled by default. The global function control is not stored in NVRAM.

Command Mode VLAN interface configuration or Global configuration

Usage Guideline Under interface configuration for an interface, the corresponding VLAN must first be created.

When the user executes the command under global configuration, it will enable/disable all existing VLAN IGMP snooping function. However the command takes effect only in the running configuration and it will not be kept in NVRAM for the next start up configuration. For a VLAN interface, the command can be kept in NVRAM for the next startup system configuration mode.

To disable IGMP snooping on a VLAN interface, use the no ip igmp snooping under VLAN interface configuration mode.

The command will, under global configuration mode, enable IGMP snooping functions for all existing VLANs. Similarly, no ip igmp snooping will disable IGMP snooping function for all of the existing VLANs.

As a VLAN is deleted, the related IGMP snooping setting for the VLAN is also removed from system configuration.

Examples

This example shows how to globally enable IGMP Snooping for all existing VLANs.

```
Switch(config)# ip igmp snooping
Switch(config)# end
Switch#
```

This example shows how to enable IGMP Snooping on VLAN1

```
Switch(config)# interface vlan1
Switch(config-if)# ip igmp snooping
Switch(config-if)# end
Switch#
```

Verfiy the settings by entering the **show ip igmp snooping** command.

ip igmp snooping (multicast router)

Use this command to configure the specified interface(s) as multicast router ports, or forbidden to be multicast router ports on the switch. Use the no form of this command to remove the interface(s) from multicast router ports, or forbidden multicast router ports.

ip igmp snooping { mrouter-designate | mrouter-not-allowed } interface *INTERFACE-ID* **[, | -]**

no ip igmp snooping { mrouter-designate | mrouter-not-allowed } interface *INTERFACE-ID* **[, | -]**

Syntax Description	
mrouter-designate	Designate a range of interfaces as being connected to multicast-enabled routers.
mrouter-not-allowed	Designate a range of interfaces as being not connected to multicast-enabled routers.
INTERFACE-ID	The interface can be a physical interface or a port-channel.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default No IGMP snooping multicast router port is configured.

Command Mode VLAN interface configuration

Usage Guideline The valid interface can be a physical port or a port-channel for the *INTERFACE-ID* parameter.

The router member port can be either dynamically learned or statically configured into an IGMP snooping entity. With dynamic learning, the IGMP snooping entity will listen to IGMP, PIM, and DVMRP packet to identify whether the partner device is a multicast router.

To add a multicast router port statically, use the **ip igmp snooping mrouter-designate** configuration. On the opposite side, it is also possible to use **ip igmp snooping mrouter-not-allowed** to configure those ports that cannot become multicast router ports even the port has received IP multicast control protocol message.

The member port of a port channel can not be enabled with the **ip igmp snooping {mrouter-designate | mrouter-not-allowed}** command, an error message is displayed if the designated port is ineligible.

Examples This example shows how to add a multicast router port on vlan1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip igmp snooping mrouter-designate interface eth3.1
Switch(config-if)# exit
Switch(config)#
```

Verfiy the settings by entering the **show ip igmp snooping mrouter** command.

This example displays a configuration error, eth3.1 (on vlan4) is not eligible to be designated as a multicast router interface for VLAN 5.

```
Switch(config)# interface vlan5
Switch(config-if)# ip igmp snooping mrouter-designate interface eth3.1
Error: eth3.1 is not vlan5 member
Switch(config-if)#exit
Switch(config)#
```

This example displays an error, the system is not allowing the configuraiton because the VLAN interface is not eligible to be designated as a multicast router interface.

```
Switch(config)# interface vlan4
Switch(config-if)# ip igmp snooping mrouter-designate interface vlan5
% Interface type not support vlan5
Switch(config-if)# exit
Switch(config)#
```

Verfiy the settings by entering the **show ip igmp snooping mrouter** command.

ip igmp snooping immediate-leave

Use this command to configure the **IGMP Snooping immediate-leave** function on VLAN interfaces. Use **no ip igmp snooping immediate-leave** to disable the immediate-leave function on the specified VLAN.

ip igmp snooping immediate-leave

no ip igmp snooping immediate-leave

Syntax None

Default Disabled

Command Mode VLAN Interface configuration

Usage Guideline The **ip igmp snooping immediate-leave** command allows IGMP Snooping membership of an interface to be removed immediately without any further confirmation mechanism (such as time out) when the interface receives an IGMP leave message from the IGMP client.

Example This example shows how to enable IGMP Snooping immediate-leave on VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)#ip igmp snooping immediate-leave
Switch(config-if)# end
```

Verfiy the settings by entering the **show ip igmp snooping** command.

ip igmp snooping querier

Use this command to enable the IGMP Snooping querier function in Layer 2 networks. Use the no form of this command to disable the function of the IGMP Snooping Querier.

ip igmp snooping querier

no ip igmp snooping querier

Syntax None

Default Disabled

Command Mode VLAN Interface configuration

Usage Guideline The system can work as the querier role when the querier for an IGMP snooping domain is enabled. If the system receives query packets from other routers, the IP address of the system and the IP address of the other routers is used to determine the final querier. The routers (network devices) with lower IP addresses become the querier.

The querier sends a general query at the interval specified by query-interval. Upon receiving the general query, the IGMP client (or host) needs to respond to the query packet in order to express that it remains in the specified group. The maximum response time instructs the client to report within the time period specified.

If the IGMP snooping entity does not receive a report from a client for a specific group after a specific time period, the port is removed from the member port list of the specific group. This specific time period is referred to as the group membership interval. The group membership interval is equal to **query-interval*** **robustness variable** + **max response time**.

The timeout period for a querier (other querier present interval) is **query-interval** * **robustness variable** + 1/2 **max response time**. The time-out period for learning of a router port is the same value as for the other querier present interval.

The query-interval value can be changed using the **ip igmp query-interval** command (defined in IGMP command document).

As IGMP is enabled on the specified VLAN of the switch, the IGMP snooping querier is suspended at the VLAN as if it were disabled, because of IGMP.

Example This example shows how to enable IGMP Snooping querier state on VLAN 1.

```
Switch> configure terminal
Switch(config)# interface vlan1
Switch(config-if)#ip igmp snooping querier
Switch(config-if)# end
Switch#
```

Verfiy the settings by entering the **show ip igmp snooping** command.

ip igmp snooping static-group

Use this command to configure an IGMP snooping static group.

Use the no form of this command to delete an IGMP snooping static group.

ip igmp snooping static-group *IP-ADDRESS* **[source** *IP-ADDRESS***] interface INTERFACE-ID [,|-]**

no ip igmp snooping static-group [*IP-ADDRESS* **[source IP-ADDRESS]**

[interface *INTERFACE-ID* **[, | -]]]**

Syntax Description	
IP-ADDRESS	The first *IP-ADDRESS* is the IP multicast group address of a group which the user would like to see. (Optional) The second *IP-ADDRESS* is the IP address of a system where multicast data packets originate.
INTERFACE-ID [, | -]	The interface or an interface list. Only a physical interface or a port-channel is allowed.

Default No static-group

Command Mode VLAN interface configuration

Usage Guideline This command applies to IGMP Snooping on a VLAN interface to statically add group membership entries and/or source records.

If a physical port is used as interface parameter for this command and it is already one member port of a port-channel then the command is aborted and an error message indicates the condition.

If the specified interface parameter (such as port or port-channel) interface does not belong to the VLAN where this command is going to apply the specified interfaces, then the system returns an error message to indicate that the command is ignored.

The command creates an IGMP snooping static group.

If an **igmp snooping static-group** configuration exists in the switch, then the switch has to respond to the IGMP query for these configured static-group addresses.

The Reserved IP multicast address 224.0.0.X must be excluded from the configured group.

The VLAN has to be created before creating an IGMP snooping static-group. When the associated VLAN is deleted, the related IGMP snooping static-group entries are also removed from system configuration.

Example The following example, on the next page, shows how to statically add group and/or source records for IGMP Snooping.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip igmp snooping static-group 226.1.2.3 interface eth3.5
Switch(config-if)# exit
Switch(config)#interface vlan1
Switch(config-if)#ip igmp snooping static-group 226.1.2.6 source 10.1.2.3
interface eth3.5
```

Verify the settings by entering the **show ip igmp snooping group** command.

ip igmp version

Use this command to change the IGMP version on the specified interface.

ip igmp version {1|2|3}

Syntax Description	
1	Configure the Switch to run IGMP version 1.
2	Configure the Switch to run IGMP version 2.
3	Configure the Switch to run IGMP version 3.

Default **3**

Command Mode VLAN interface configuration

Usage Guideline If the IGMP interface version is configured to a lower version, then the higher version IGMP Report/Leave messages are ignored.

This version will apply to both IGMP and IGMP snooping operation.

Example This example shows how to configure IGMP version. It configures the IGMP version to 3.

```
Switch# configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ip igmp version 3
Switch(config-if)# end
```

Verify the settings by entering the **show ip igmp interface** command.

ip mroute

Use this command to create a multicast static route (mroute).

Use the no form of this command to delete the route.

ip mroute *SOURCE-NETWORK* **{** *RPF-ADDRESS* **| Null }** **[** *DISTANCE* **]**

no ip mroute *SOURCE-NETWORK*

Syntax Description	
SOURCE-NETWORK	Network address of the multicast source. Format: A.B.C.D/M.
RPF-ADDRESS	RPF neighbor address for the multicast route.
Null	Indicates Null interface. When set to Null, the RPF check result will always be failed.
DISTANCE	(Optional) Specifies whether a unicast route or multicast static route is used for the RPF lookup. Lower distances have preference. If the multicast static route has the same distance as the other RPF sources, the multicast static route takes preference. Default is 0. Range is 0-255.

Default DISTANCE: 0

Command Mode Global configuration

Usage Guideline This command statically configures where multicast sources are located even when the unicast routing table shows something different.

If the RPF-ADDRESS is a PIM neighbor, PIM join, graft, and prune messages are sent to it.

Examples The following example configures the multicast data source within network 192.168.6.0/24 to be accessible with the neighbor router 10.1.1.1.

```
Switch(config)#ip mroute 192.168.6.0/24 10.1.1.1
```

The following example configures the multicast data source within network 192.168.7.0/24 to be accessible with the neighbor router 10.1.1.1 and with the distance value of 100.

```
Switch(config)#ip mroute 192.168.7.0/24 10.1.1.1 100
```

The following example configures the multicast data source within a network number 192.168.8.0/24 to be discarded.

```
Switch(config)#ip mroute 192.168.8.0/24 null
```

The following example removes a previously configured ip mroute entry of 192.168.8.0/24.

```
Switch(config)#no ip mroute 192.168.8.0/24
```

Verify the settings using the **show running-config** command.

ip mtu

Use this command to set the MTU value in TCP/IP stack. Use the default form to restore to the default ip mtu size.

ip mtu *BYTES*

default ip mtu

Syntax Description	
BYTES	Set the IP MTU value in TCP/IP stack. The range is 1280 to 9692 bytes.

Default 1500 bytes

Command Mode VLAN interface configuration

Usage Guideline IP packets sent by the device will be fragmented based on this value.

Some routing protocols, such as OSPF, will use this value to advertise routing updates.

Examples This example shows how to set ip mtu as 6000 bytes at vlan 4.

```
Switch# configure terminal
Switch(config)# interface vlan4
Switch(config-if) ip mtu 6000
Switch(config-if)# end
```

This example shows how to restore the default ip mtu.

```
Switch# configure terminal
Swtich(config)# interface vlan4
Switch(config-if)# default ip mtu
Switch(config-if)# end
```

Verify the settings by entering the **show interface** command.

ip mtu (management port)

Use this command to set the IP layer maximum transfer unit of the Management Port. Use no form command to reset to the default ip mtu.

ip mtu *BYTES*

no ip mtu

Syntax Description	
BYTES	The maximum transfer unit in bytes. The range is 1500 to 9180 bytes.

Default 1500 bytes

Command Mode Management interface configuration

Usage Guideline IP packets sent by the device will be fragmented based on this value.

Example This example shows how to set the ip mtu of the Management Port to 1600 bytes.

```
Switch#configure terminal
Switch(config)#mgmt-if
Switch(mgmt-if)#ip mtu 1600
Switch(mgmt-if)#end
```

Verify the settings by entering the **show mgmt-if** command

ip multicast-routing

Use this command to enable IP multicast routing. Use the no form of this command to disable IP Multicast routing.

ip multicast-routing

no ip multicast-routing

Syntax None

Default Disabled

Command Mode Global configuration

Usage Guideline If the **no ip multicast-routing** command is used, the device stops routing multicast packets even when the protocols are enabled.

Example This example shows how to enable IP multicast routing.

```
Switch(config)# ip multicast-routing
```

Verify the settings by the **show system protocol-state** command.

ip ospf authentication

Use this command to send and receive OSPF packets with the specified authentication method. Use the no form of this command to disable the authentication.

ip ospf authentication [message-digest]

no ip ospf authentication

Syntax Description	
message-digest	(Optional) Use the message digest authentication.

Default No authentication

Command Mode Interface configuration

Usage Guideline The authentication mode can be: no-authentication, use authentication key for authentication, or use message-digest key for authentication.

When it is specified to use the authentication key but the key is not configured, then null key will be used.

When it is specified to use the message digest but the digest key is not configured, then the null key will be used.

Example In the following example shows how to enable message authentication on interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf message-digest-key 10 md5 yourpass
Switch(config-if)# ip ospf authentication message-digest
```

Verify the settings by entering the **show ip ospf interface** command.

ip ospf authentication-key

Use this command to specify an OSPF authentication password for the neighboring routers. Use the no form of this command to remove an OSPF authentication password.

ip ospf authentication-key *PASSWORD*

no ip ospf authentication-key

Syntax Description	
PASSWORD	Specifies the authentication password. Any continuous string of characters that can be entered from the keyboard up to 8 bytes in length. The syntax is a general string that does not allow spaces.

Default None

Command Mode Interface configuration

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. All neighboring routers on the same network with the same password exchange OSPF routing data.

Use the ip ospf authentication command to enable authentication. Simple password authentication allows a password to be configured for each interface. Configure the routers in the same routing domain with the same password.

Example In the following example, an authentication key test is created on interface VLAN 1 in area 0. Note that first authentication is enabled for area 0.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf  authentication-key test
Switch(config-if)# ip ospf authentication
```

Verify the settings by entering the **show ip ospf interface** command

ip ospf cost

Use this command to explicitly specify the cost of sending a packet on an interface. Use the no form of the command to remove the assignment.

ip ospf cost *COST*

no ip ospf cost

Syntax Description	
COST	Specifies the value of the link-state metric. The range is 1 to 65535.

Default Cost is not configured

Command Mode Interface configuration

Usage Guideline The interface cost indicates the overhead required to send packets across a certain interface. This cost is advertised as the link cost in the router link advertisement. The cost is inversely proportional to the bandwidth of an interface. The cost can be either manually assigned or be automatically determined.

By default, the cost of an interface is calculated based on the bandwidth (10E8 / bandwidth); use the **ip ospf cost** command to set the cost manually.

If the cost is explicitly assigned, the assigned cost will override the auto-determined cost. Otherwise, the auto-determined cost will be adopted.

Example The following example shows sets the interface cost value to 10 on interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf cost 10
```

Verify the settings by entering the **show ip ospf interface** command.

ip ospf dead-interval

Use this command to set the interval during which no hello packets are received and after which a neighbor is declared dead. The no form of this command will reset the dead-interval to the default value.

ip ospf dead-interval *SECONDS*

no ospf dead-interval

Syntax Description	
SECONDS	Specifies the interval in seconds. The range is 1 to 65535.

Default 40 seconds

Command Mode Interface configuration

Usage Guideline The dead-interval is the amount of time that the router waits to receive an OSPF hello packet from a 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.

Specifying a smaller dead interval in seconds will give faster detection of a neighbor being down and improve convergence, but it may cause additional routing instability.

Example The following example shows configuring dead-interval to 10 seconds on VLAN 1 interface.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf dead-interval 10
```

Verify the settings by entering the **show ip ospf interface** command.

ip ospf hello-interval

Use this command to specify the interval between hello packets. The no-form of this command will reset the hello-interval to the default value.

ip ospf hello-interval *SECONDS*

no ip ospf hello-interval

Syntax Description	
SECONDS	Specifies the interval in seconds. The range is 1 to 65535.

Default 10 seconds

Command Mode Interface configuration

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 results in more routing traffic.

When configuring the hello-interval, if the hello-interval*4<= 65535, then the dead-interval will be automatically updated to hello-interval*4.

Example The following example shows setting the hello-interval to 3 seconds on interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf hello-interval 3
```

Verify the settings by entering the **show ip ospf interface** command.

ip ospf message-digest-key

Use this command to register an MD5 key for OSPF MD5 authentication.

Use the no form of this command to remove an MD5 key.

ip ospf message-digest-key *KEY-ID* **md5** *KEY*

no ip ospf message-digest-key *KEY-ID*

Syntax Description	
KEY-ID	Specifies a value for key identifier. The range is 1 to 255.
KEY	Specifies the OSPF password. The syntax is a general string, 1-16 characters with no spaces.

Default None

Command Mode Interface configuration

Usage Guideline Message Digest Authentication is a cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the OSPF packet, the key, and the *KEY-ID* to generate a message digest that gets appended to the packet. Use this command for uninterrupted transitions between passwords. This is helpful for administrators who want to change the OSPF password without disrupting communication. The system begins a rollover process until all the neighbors have adopted the new password. This allows neighboring routers to continue communication while the network administrator is updating them with a new password. The router will stop sending duplicate packets once it detects that all of its neighbors have adopted the new password.

Maintain only one password per interface, removing the old password whenever a new one is added. This prevents the local system from continuing to communicate with the system that is using the old password. Removing the old password also reduces overhead during rollover. All neighboring routers on the same network must have the same password value to enable exchange of OSPF routing data.

Example The following example shows how to set a new key 10 with password *yourpass* on interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf authentication message-digest
Switch(config-if)# ip ospf message-digest-key 10 md5 yourpass
```

Verify the settings by entering the **show ip ospf interface** command.

ip ospf priority

Use this command to set the router priority to determine the designated router for the network. The no form of this command will reset the priority to the default value.

ip ospf priority *PRIORITY*

no ip ospf prority

Syntax Description	
PRIORITY	Specifies the priority of the router on the interface. The range is 0 to 255.

Default *PRIORITY*: 1

Command Mode Interface configuration

Usage Guideline Set the priority to help determine the OSPF Designated Router (DR) for a network. If two routers attempt to become the DR, the router with the higher router priority becomes the DR. If the router priority is the same for two routers, 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. Configure router priority for multi-access networks (not point-to-point) only.

Example The following example shows setting the OSPF priority value to 3 on VLAN 1 interface.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf priority 3
```

Verfiy the settings by entering the **show ip ospf interface** command.

ip ospf retransmit-interval

Use this command to specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The no form of this command will reset the retransmit-interval to the default value.

ip ospf retransmit-interval *SECONDS*

no ip ospf retransmit-interval

Syntax Description	
SECONDS	Specifies the interval in seconds. The range is 1 to 65535.

Default 5 seconds

Command Mode Interface configuration

Usage Guideline After sending an LSA to a neighbor, the router keeps the LSA until it receives an acknowledgement. In case the router does not receive an acknowledgement during the set time (the retransmit interval value) it retransmits the LSA. Set the retransmission interval value conservatively to avoid needless retransmission. The interval should be greater than the expected round-trip delay between two routers.

Example The following example shows setting the ospf retransmit interval to 10 seconds on sVLAN 1 interface

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf retransmit interval 10
```

Verfiy the settings by entering the **show ip ospf interface** command

ip ospf shutdown

To initiate a graceful shutdown of Open Shortest Path First (OSPF) protocol at interface level, use the **ip ospf shutdown** command in router configuration mode. To restart the OSPF protocol on an interface, use the no form of this command.

ip ospf shutdown [*IFNAME* **]**

no ip ospf shutdown [*IFNAME* **]**

Syntax Description	
IFNAME	(Optional) Specifies a layer 3 interface. If no option is specified, the command applies to the entire OSPF process.

Default None

Command Mode Router configuration

Usage Guideline Use the **ip ospf shutdown** command to place the OSPF protocol, on a specific interface, into shutdown mode.

If no interface is specified with this command, the entire protocol will shutdown in the least disruptive manner and notify its neighbors that it is not available.

Traffic that can follow another route through the network, will be directed to that alternate path.

Example The following example shows how to initiate an OSPF protocol shutdown on the layer 3 interface (VLAN 1):

```
Switch(config)# router ospf
Switch(config-router)# ip ospf shutdown vlan1
```

ip ospf transmit-delay

Use this command to set the estimated time it takes to transmit a link-state-update packet on the interface.

Use the no parameter with this command to return to the default value.

ip ospf transmit-delay *SECONDS*

no ip ospf transmit-delay

Syntax Description	
SECONDS	Specifies the interval in seconds. The range is 1 to 65535.

Default 1 second

Command Mode Interface configuration

Usage Guideline The transmit delay value adds a specified time to the age field of an update. If the delay is not added, the time in which the LSA transmits over the link is not considered. This command is especially useful for low speed links. Remember to add transmission and propagation delays when setting the transmit delay value.

Example The following example shows setting the OSPF transmit delay to 10 seconds on the VLAN 1 interface.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf transmit delay 10
```

Verify the settings by entering the **show ip ospf interface** command.

ip ospf mtu-ignore

To disable OSPF MTU mismatch detection on receiving DBD packets, use the ip ospf mtu-ignore command in interface configuration mode. To reset to default, use the no form of this command.

ip ospf mtu-ignore

no ip ospf mtu-ignore

Syntax Description None

Default OSPF MTU mismatch detection is enabled.

Command Mode Interface configuration

Usage Guideline OSPF checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange Database Descriptor (DBD) packets. If the receiving MTU in the DBD packet is higher than the IP MTU configured on the incoming interface, OSPF adjacency will not be established.

Example The following example disables MTU mismatch detection on receiving DBD packets.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf mtu-ignore
```

ip pim

Enable PIM on the interface for either sparse mode or dense mode operation. Use the no form of the command to disable the PIM function on the interface.

ip pim {sparse-mode | dense-mode}

no ip pim {sparse-mode | dense-mode }

Syntax Description	
sparse-mode	Enables sparse mode of operation.
dense-mode	Enables dense mode of operation.

Default IP multicast routing is disabled on all interfaces.

Command Mode Interface configuration.

Usage Guideline This command is only valid for the VLAN interface.

Use this command to specify the PIM operating mode for an interface. The interface can be either operated in the sparse mode or the dense mode.

To switch the PIM operating mode please use no ip pim {sparse-mode | dense-mode} to disable PIM at first then set the new mode required. PIM needs to be disabled first since only one multicast routing protocol can be enabled on one interface. When the command **ip pim dense-mode** is issued, PIM dense mode will be configured on the interface. Therefore when the command **ip pim sparse-mode** is issued, attempting to execute sparse mode on the interface, the system will reply with an error message because PIM dense mode is already configured on that interface.

Enabling PIM on an interface also enables Internet Group Management Protocol (IGMP) operation on that interface.

Before the PIM function is enabled on an interface, enable IP multicast routing by issuing the command **ip multicast-routing** in global configuration mode.

Example This example shows how to enable PIM-SM protocol on a specified interface.

```
Switch(config)# interface vlan1
Switch(config-if)# ip pim sparse-mode
```

Verify the settings by entering the **show ip pim interface** command.

ip pim accept-register

To configure a candidate rendezvous point (RP) router to filter PIM register messages, use the ip pim accept-register command in global configuration mode. To disable this function, use the no form of this command.

ip pim accept-register source-list *ACCESS-LIST-NAME*

no ip pim accept-register

Syntax Description	
source-list *ACCESS-LIST-NAME*	Specifies the name of the basic IP access list name.

Default Disabled

Command Mode Global configuration

Usage Guideline This command can be only specified once. The later applied command will override the previous setting.

Use this command to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the RP will immediately send back a register-stop message.

Example The following example shows how to restrict the RP from allowing sources in the Source Specific Multicast (SSM) range of addresses to register with the RP. These statements need to be configured only on the RP.

```
Switch# configure terminal
Switch(config)# ip access-list Summer-Movie
Switch(config-ip-acl)# deny any 232.0.0.0 255.0.0.0
Switch(config-ip-acl)# permit any any
Switch(config-ip-acl)# exit
Switch(config)# ip pim accept-register source-list Summer-Movie
```

Verify the settings by the **show ip pim** command.

ip pim bsr-candidate

Use this command to configure the router to advertise itself as a candidate bootstrap router (BSR). Use the no form of this command to remove this router as a candidate for being a BSR.

ip pim bsr-candidate *INTERFACE-ID [HASH-MASK-LENGTH] [PRIORITY]*

no ip pim bsr-candidate

Syntax Description	
INTERFACE-ID	Interface ID, from which the BSR address is derived, in order to make it a candidate.
HASH-MASK-LENGTH	Configure hash mask length for RP selection. The range is 0 to 32. The mask (32 bits maximum) that is to be logically ANDed with the group address before the hash function is executed. All groups with the same seed hash (correspond) to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. Therefore one RP can be derived for multiple groups.
PRIORITY	Configure priority for a BSR candidate. The range is 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR.

Default The router is not a BSR candidate.

HASH-MASK-LENGTH: 30

Priority : 64.

Command Mode Global configuration

Usage Guideline This command is valid in the SM mode

This command causes the router to send bootstrap messages to all its PIM neighbors, with the address of the designated interface as the BSR address.

The following 2 conditions will cause BSR changes:

(1) Bootstrap Timer Expires

(2) Receive Preferred BSM.

In condition (1), the router is a Candidate-BSR, it will start to originate Bootstrap messages and perform the BSR election. For condition (2), the router will store the RP-Set from the preferred BSR.

Functionality of hash-mask is defined in RFC4601 4.7.2. The hash function 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 (all of this set has the same longest mask length and the 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.

Example

The following example shows how to configure the IP address of the router on VLAN 1 to be a candidate BSR with hash-mask length of 20 and priority of 192:

```
Switch(config)# ip pim bsr-candidate vlan1 20 192
Switch(config)#
```

Verify the settings by using the **show ip pim** command.

ip pim dr-priority

Use this command to change the Designated Router Priority value inserted into the DR Priority option of the PIM Hello message. Use default command to return the setting to default.

ip pim dr-priority *PRIORITY*

default ip pim dr-priority

Syntax Description	
PRIORITY	The value of DR priority in the range of 0 to 4294967295. A larger value of this argument means a higher priority.

Default PRIORITY: 1

Command Mode VLAN interface configuration

Usage Guideline This command is only valid for the VLAN interface.

This command is only effective for the SM mode.

When a DR is a candidate for election, the following conditions apply:

- The router with the highest priority value configured on an interface will be elected as the DR. If this priority value is the same on multiple routers, then the router with the highest IP address configured on an interface will be elected as the DR.
- If a router does not advertise a priority value in its hello messages, the router is regarded as having the highest priority and will be elected as the DR. If there are multiple routers with this priority status, then the router with the highest IP address configured on an interface will be elected as the DR.

Example The following example sets the DR priority of the vlan 1 interface to 200.

```
Switch(config)# interface vlan1
Switch(config-if)# ip pim dr-priority 200
```

Verify the settings by entering the **show ip pim interface** command.

ip pim join-prune-interval

Use this command to configure a Join/Prune interval value different from the default (60 seconds).

ip pim join-prune-interval *SECONDS*

Syntax Description	
SECONDS	The number of seconds that can be configured for the interval between Join/Prune messages. The range is 1 to 18000.

Default 60 seconds

Command Mode VLAN interface configuration

Usage Guideline This command is only valid for the VLAN interface.

This command is valid for SM only.

When configuring 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 (for example, 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, the 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 no join message is received on this interface.

Example The following example changes the PIM Join/Prune timer to 120 seconds.

```
Switch(config)# interface vlan1
Switch(config-if)# ip pim join-prune-interval 120
```

Verify the settings by entering the **show ip pim interface** command.

ip pim prune-limit-interval

Use this command to configure the time interval for the prune limit timer to limit the Pruning rate on a LAN.

ip pim prune-limit-interval *SECONDS*

Syntax Description	
SECONDS	Specifies the value of Prune Limit Timer (in seconds), which is used to prevent Prune storms on a LAN. The range is 1 to 18000.

Default 210 seconds

Command Mode VLAN interface configuration

Usage Guideline This command is only valid for the VLAN interface.

This command is valid for PIM-DM only.

This interval is used to configure prune-limit-timer which limits the Pruning rate on a LAN. It is only used when the Upstream(S,G) state machine is in the Pruned state. A Prune cannot be sent if this timer is running. This timer is normally set to default value 210 seconds.

Example The following example configures interface VLAN 1 with the PIM prune limit timer interval set to 120 seconds.

```
Switch(config)# interface vlan1
Switch(config-if)# ip pim prune-limit-interval 120
```

Verify the settings by entering the **show ip pim interface** command.

ip pim query-interval

Use this command to configure the frequency of PIM hello message.

ip pim query-interval *SECONDS*

Syntax Description	
SECONDS	The number of seconds that can be configured for the interval between Hello messages. The range is 1 to 18000.

Default 30 seconds

Command Mode VLAN interface configuration

Usage Guideline This command is only valid for the VLAN interface.

This command is valid for both SM and DM.

A PIM router learns PIM neighbors via the hello message.

Routers configured for IP multicast send PIM hello messages to detect PIM routers. For SM, hello messages are also used to determine which router will be the designated router for each LAN segment.

If the router has interfaces operating in the SM mode, the designated router will send Registration messages to the rendezvous point (RP).

Example The following example changes the PIM hello interval to 45 seconds.

```
Switch(config)# interface vlan1
Switch(config-if)# ip pim query-interval 45
```

Verify the settings by entering the **show ip pim interface** command.

ip pim register-checksum-include-data

Use this command to configure the option to calculate the Register checksum over the whole packet. Use the no form of this command to disable calculating the Register checksum over the whole packet.

ip pim register-checksum-include-data { group-list *ACCESS-LIST-NAME***}**

no ip pim register-checksum-include-data

Syntax Description	
group-list *ACCESS-LIST-NAME*	Specifies the name of the basic IP access list name

Default Disabled

By default, the Register Checksum is calculated only over the header.

Command Mode Global configuration

Usage Guideline This command is valid for SM mode and used to provide compatible inter-operability with other manufacturer devices per the following:

This command is used to inter-operate with some legacy *CISCO*® manufactured routers using older *CISCO*® *IOS*™ versions. This command is needed for the first hop router for encapsulation of the register packet. This function needs to be enabled in order to inter-operate with legacy *CISCO*® devices using older *IOS*™ versions.

If group-list is not specified, then the setting will be applied to all groups.

This command can be only specified once. The later applied command will override the previous setting.

Example The following example shows how to enable register checksum over whole packet.

```
Switch(config)# ip pim register-checksum-include-data
```

Verify the settings by using the **show ip pim** command.

ip pim register-suppresion

Use this command to configure the register-suppression time.

ip pim register-suppression *SECONDS*

Syntax Description	
SECONDS	Register suppression time-out value in seconds. The range is 11 to 255.

Default 60 seconds

Command Mode Global configuration

Usage Guideline This command is valid for SM mode.

When a DR receives the register-stop message, it will start the suppression timer. During the suppression time a DR will stop sending Register-encapsulated data to the RP.

This timer should be configured on the designated router.

Note: the parameter Register Probe Time in RFC 4601 is fixed to 5 (not configurable). It 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.

Example This example shows how to configure the register-suppression time to 30 seconds.

```
Switch(config)# ip pim register-suppression 30
```

Verify the settings by the **show ip pim** command.

ip pim rp-address

Use this command to statically configure the rendezvous point (RP) address for multicast groups. To remove an RP address, use the no form of this command.

ip pim rp-address *IP-ADDRESS* **[group-list** *ACCESS-LIST-NAME***] [override]**

no ip pim rp-address *IP-ADDRESS*

Syntax Description	
IP-ADDRESS	IP address of a router to be a PIM RP.
group-list *ACCESS-LIST-NAME*	(Optional) Specifies the name of multicast ACCESS-LIST for which multicast groups that the RP should use. If the access-list is not specified, the default multicast group is 224.0.0.0/4.
override	(Optional) When there is a conflict between static RP configuration and the information learned by BSR, static RP configuration has the higher priority than the BSR learned information.

Default None

Command Mode Global configuration

Usage Guideline This command is only valid for SM mode.

Use this command to statically define the RP address for multicast groups that are to operate in sparse mode.

A User can use a single RP for more than one group. The conditions specified by the access list determine which groups that the RP can use. A PIM router can define multiple RPs, but only one RP can be defined per multicast group.

To configure the static-RP function in the PIM SM domain, this command needs to be configured across all of the routers in the PIM domain.

Multiple RP addresses can be specified by the command. Only one access-list can be specified for an RP. The new setting overrides the old one.

Example The following example sets the PIM RP address to 10.90.90.90 for multicast group 225.2.2.2 only:

```
Switch(config)# ip access-list PIM-Control
Switch(config-ip-acl)# permit any host 225.2.2.2
Switch(config-ip-acl)# exit
Switch(config)# ip pim rp-address 10.90.90.90 group-list PIM-Control
```

Verify the settings by using the **show ip pim** command.

ip pim rp-candidate

Use this command to configure the router as an RP candidate. Use the no form of this command to remove the router as a candidate RP.

ip pim rp-candidate *INTERFACE-ID* **[group-list** *ACCESS-LIST-NAME* **] [interval** *SECONDS***] [priority** *PRIORITY***]**

no ip pim rp-candidate [*INTERFACE-ID* **]**

Syntax Description	
INTERFACE-ID	Specifies the interface ID. The IP address associated with this interface is advertised as a candidate RP address.
group-list *ACCESS-LIST-NAME*	(Optional) Specifies the name of the multicast access list that defines the group prefixes that are advertised in association with the RP address. If no group-list is specified, the switch is a candidate RP for all groups.
interval *SECONDS*	(Optional) Indicates the RP candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.
priority *PRIORITY*	(Optional) Indicates the RP priority value. The range is from 0 to 255. The default value is 192.

Default

The router is not an RP candidate by default.

interval: 60 seconds

priority: 192

Command Mode

Global configuration

Usage Guideline

This command is valid for SM mode.

Only one group access list can be specified for the command.

The command can be applied multiple times, each for a different interface.

This command causes the router to send a PIM Version 2 message advertising itself as a candidate RP to the BSR.

Use this command only in backbone routers that have good connectivity to all parts of the PIM domain. That is, a stub router that relies on an on-demand dialup link to connect to the rest of the PIM domain is not a good candidate RP.

Example

The following example (on the next page) shows how to configure the router to advertise itself as a candidate RP to the BSR in its PIM domain. A basic IP

access list, named PIM-Control, which specifies the group prefix (239.0.0.0/8), is associated with the RP that has the address identified by VLAN interface 1 and with priority 3.

```
Switch(config)# ip access-list PIM-Control
Switch(config-ip-acl)# permit any 239.0.0.0 255.0.0.0
Switch(config-ip-acl)# exit
Switch(config)# ip pim rp-candidate vlan1 group-list PIM-Control priority 3
```

Verify the settings by using the **show ip pim** command.

ip pim state-refresh origination-interval

Configure a PIM-DM State-Refresh origination interval different from the default value (60 seconds). The origination interval is the number of seconds between PIM-DM State Refresh control messages.

ip pim state-refresh origination-interval *SECONDS*

Syntax Description	
SECONDS	The number of seconds that can be configured for the interval between state-refresh messages. The range is 4 to 100.

Default 60 seconds

Command Mode Interface configuration

Usage Guideline This command is valid for the DM mode.

Configure this command on the first hop, PIM dense mode routers that are directly connected to sources for PIM-DM multicast groups.

The purpose of this message is to reduce overhead spent on the cycle in flooding and pruning of traffic. For each state-refresh origination interval, the first-hop router will initiate this message and send it to the down-stream hops. Thus, the down-stream routers can do an action similar to prune. On receiving this prune, the upstream will refresh the Prune timer, and thus not flood the traffic to the corresponding interfaces.

Example The following example sets the State Refresh Origination Interval to 100 seconds.

```
Switch(config)# interface vlan1
Switch(config-if)# ip pim state-refresh origination-interval 100
```

Verify the settings by entering the **show ip pim** interface command.

ip policy route-map

Use the command to specify a route map as the routing policy on an interface,. To disable policy routing on the interface, use the no form of this command.

ip policy route-map *MAP-NAME*

no ip policy route-map [*MAP-NAME***]**

Syntax Description

MAP-NAME	Specify the name of the route map to be used for routing policy.

Default Policy routing is disabled.

Command Mode Interface configuration mode.

Usage Guideline The command is only available for VLAN interface configuration.

The user can specify one route map as the routing policy on an interface. The policy will be applied to packets received by the interface.

Use the **match ip-address** command in route map to define the matching criteria for packets with specific characteristics. If IP access list is used with the **match ip-address** command, all of the matching criteria in the access list will be checked. The packet that matches that permit statement will be acted based on the route map. The packet that is denied by the access list will be routed based on routing table.

Use the following set command to define the action to take for policy based routing:

set ip precedence

set interface

set ip next-hop

set ipv6 next-hop

set default interface

set ip default next-hop

set ipv6 default next-hop

Examples The following example set up routing policy to route the packets that match the IP access list name pbr-acl to next-hop 20.1.1.254

```
Switch(config)#route-map pbr-map

Switch(config-route-map)# match ip address pbr-acl
Switch(config-route-map)# set ip next-hop 20.1.1.254
Switch(config-route-map)# exit
Switch(config)#
Switch(config)#interface vlan100
Switch(config-if)#ip policy route-map pbr-map
Switch(config-if)#exit
```

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

ip rip authentication key-chain

Use this command to enable authentication for RIP Version 2 packets and to specify the key that can be used on an interface. To prevent authentication, use the no form of this command.

ip rip authentication key-chain *NAME-OF-KEY*

no ip rip authentication key-chain

Syntax Description	
NAME-OF-KEY	Enables authentication and specifies the key that are valid.

Default No authentication is provided for RIP packets.

Command Mode Interface configuration

Usage Guideline If no key is configured with the **key-chain** command, no authentication is performed on the interface.

This command also specifies that the interface will use the key chain for authentication.

Example

The following example configures a key chain named chain1. Key1 named "forkey1string" will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. Key3 named "forkey3string" will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m.

```
Switch(config)# interface vlan1
Switch(config-if)# ip rip authentication key-chain chain1
Switch(config-if)# ip rip authentication mode text
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 172.19.0.0/8
Switch(config-router)# version 2
Switch(config-router)# exit
Switch(config)# key chain chain1
Switch(config-keychain)# key 1
Switch(config-keychain-key)# key-string forkey1string
Switch(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2009 duration 7200
Switch(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2009 duration 3600
Switch(config-keychain-key)# exit
Switch(config-keychain)# key 3
Switch(config-keychain-key)# key-string forkey3string
Switch(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2009 duration 7200
Switch(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2009 duration 3600
Switch(config-keychain-key)# exit
```

Verify the settings by entering the **show ip protocols rip** command.

ip rip authentication mode

To configure the type of authentication used in Routing Information Protocol (RIP) Version 2 packets, use the **ip rip authentication mode** command in interface configuration mode. Use the no form of the command to disable the authentication function.

ip rip authentication mode { text | md5 }

no ip rip authentication mode

Syntax Description	
text	Clear text authentication.
md5	Keyed Message Digest 5 (MD5) authentication.

Default Clear text authentication (**text**)

Command Mode Interface configuration

Usage Guideline Only VLAN interfaces at which IP addresses are configured are valid interfaces for this command.

RIP Version 1 does not support authentication. This command only affects RIPv2.

Example The following example shows how to configure the authentication mode of the interface to **md5** at interface VLAN 2:

```
Switch(config)# interface vlan2
Switch(config-if)# ip rip authentication mode md5
```

Verify the settings by entering the **show ip rip interface** command.

ip rip receive version

Use this command to specify a RIP version to receive on each interface. Use the no form of the command to let the version follow the setting specified in the router configuration mode.

ip rip receive version *VERSION-ID* **[, | -]**

no ip rip receive version

Syntax Description	
VERSION-ID	The *Version ID* can be either 1 or 2. That is RIP accepts only RIP Version 1 packets on the interface or accepts only RIP Version 2 packets on the interface. It also can be a list of version IDs such as 1,2 (or 1-2), meaning that both RIP Version 1 and Version 2 packets are acceptable on the RIP enabled interface.

Default Global RIP version receive setting

Command Mode Interface configuration

Usage Guideline This command applies only to the interface being configured.

Examples The following example shows how to configure interface (VLAN 1) to accept both RIP Version 1 and Version 2 packets:

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip rip receive version 1-2
Switch(config-if)# end
```

The following example shows how to configure the interface (VLAN 1) to only accept RIP Version 1 packets:

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip rip receive version 1
Switch(config-if)# end
```

Verify the settings by entering the **show ip rip interface** command.

ip rip send version

Use this command to specify a RIP version to send on an interface basis. Use the no form of the command to let the version following the setting specified in the router configuration mode.

ip rip send version *VERSION-ID* **[, | -]**

no ip rip send version

Syntax Description	
VERSION-ID	The RIP *Version ID* can be either 1 or 2. That is, send out only RIP Version 1 packets on the interface or send out only RIP Version 2 packets on the RIP enabled interface. It also can be a list of version IDs such as 1,2 (or 1-2) meaning that both RIP Version 1 and Version 2 packets can be sent out from the RIP enabled interface.

Default Global RIP version transmitt setting

Command Mode Interface configuration

Usage Guideline This command applies only to the interface being configured.

Examples The following example shows how to configure the interface (VLAN 100) to send both RIP Version 1 and Version 2 packets:

```
Switch# configure terminal
Switch(config)# interface vlan100
Switch(config-if)# ip rip send version 1,2
Switch(config-if)# end
```

The following example shows how to configure the interface (VLAN 100) to send only RIP Version 2 packets:

```
Switch# configure terminal
Switch(config)# interface vlan100
Switch(config-if)# ip rip send version 2
Switch(config-if)# end
```

Verify the settings by entering the **show ip rip interface** command.

ip rip v2-broadcast

Use this command to allow Routing Information Protocol (RIP) Version 2 update packets to be sent as broadcast packets instead of multicast packets, Use the no form of the command to go back to multicast sending of the packet.

ip rip v2-broadcast

no ip rip v2-broadcast

Syntax None

Default Disabled

The RIPv2 update packets are to be sent as multicast packets.

Command Mode Interface configuration

Usage Guideline Use the **ip rip v2-broadcast** command to broadcast RIP Version 2 broadcast updates to hosts that do not listen to multicast broadcasts. Version 2 updates (requests and responses) will be sent to the IP broadcast address (e.g. 10.70.89.255) 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 broadcasts, the system uses an IP multicast address for periodic broadcasts. The IP multicast address is 224.0.0.9.

This command applies only to the interface being configured.

Example The following example shows how to configure the interface (VLAN 100) to broadcast Version 2 RIP packets:

```
Switch# configure terminal
Switch(config)# interface  vlan100
Switch(config-if)# ip rip send version 2
Switch(config-if)# ip rip v2-broadcast
Switch(config-if)# end
```

Verify the settings by entering the **show ip rip interface** command.

ip route

Use **ip route** to add a static route entry. Use the no form of the command to remove a static route entry.

ip route *{NETWORK-PREFIX NETWORK-MASK | NETWORK-PREFIX/PREFIX-LENGTH} IP-ADDRESS* **[distance** *DISTANCE***]**

no ip route *{NETWORK-PREFIX NETWORK-MASK | NETWORK-PREFIX/PREFIX-LENGTH} [IP-ADDRESS]*

Syntax Description	
NETWORK-PREFIX NETWORK-MASK	The network prefix and the network mask specify the destination network.
NETWORK-PREFIX/ PREFIX-LENGTH	The network prefix and the prefix length specify the destination network.
IP-ADDRESS	IP address of the next hop that can be used to reach destination network.
distance DISTANCE	(Optional) An administrative distance. The default administrative distance for a static route is 1. The range of distance is 1 to 255. The lower value represents a better route.

Default No static routes are configured.

Command Mode Global configuration

Usage Guideline When an administrative distance is specified, it flags a static route that can be overridden by dynamic information.

When the *NETWORK -PREFIX* is 0.0.0.0 and the *NETWORK -MASK* is 0, then the command will create a static default route.

The distances of routes are used in the following ways:

In single path mode, the route with the best distance will be the active route if multiple routes can reach the same destination. If multiple routes are equidistant, then one of them must be chosen as the active route.

For the single path mode, the route with the best distance and route type is selected as the primary, (active path) the other distances are available as backup paths. The active path is always considered the path with the best route type selected from the reachable paths with the best distance.

Examples This example shows how to add static default route entry with next-hop 10.1.1.254:

```
Switch(config)# ip route 0.0.0.0/0 10.1.1.254
```

Verify the settings by entering the **show ip route** command.

ip route multi-path

Use ip route multi-path to enable multiple paths for same route. Use the no form of the command to disable multiple paths.

ip route multi-path

no ip route multi-path

Syntax Description None

Default Enabled

Command Mode Global configuration

Usage Guideline If there are multiple routes with the same network-prefix co-existing, specify the route operation mode (multi-path or not) to select the routes that will be active.

For the no command, it disables the multiple path function. Only one of the multiple paths will be active.

Note: The active path may change from one path to the other under multiple paths mode, as long as the available route with a greater priority becomes reachable.

Examples This example shows how to enable multiple paths function.

```
Switch(config)# ip route multi-path
```

This example shows how to disable multiple paths function.

```
Switch(config)# no ip route multi-path
```

Verify the settings by entering the **show ip route summary** command.

ip ssh

Use this command to configure Secure Shell (SSH) control parameters or enable the SSH service on the switch. Use the **no ip ssh** command to disable the SSH service.

ip ssh [timeout *SECONDS* **| authentication-retries** *NUMBER* **| service-port** *TCP-PORT* **]**

no ip ssh

Syntax Description	
timeout *SECONDS*	(Optional) The time interval that the switch waits for the SSH client to respond. The range is 120-600. The SSH session will be closed when the session has been idle for this timeout period.
authentication-retries *NUMBER*	(Optional) The number of authentication attempts after which the session is reset or authentication failed. The range is 2-20.
service-port *TCP-PORT*	Optional) Specifies the service port, such as TCP port 22, to which Secure Shell (SSH) needs to connect. TCP ports are numbered between 1 and 65535.

Default

Initial SSH service: Disabled

timeout: 120 seconds.

Maximum **authentication retries**: 3

service port: 22

Command Mode

Global configuration

Usage Guideline

The command configures Secure Shell (SSH) server parameters on the switch.

The idle timer ("timeout" option) is refreshed when the SSH client sends the message to the server. When the idle timer expires and the SSH server does not receive any messages from the client, the session will be released.

The SSH server can be configured with extra authentication retries for setting up an SSH session. The connection will be failed when the number of authentication attempts equals the maximum number of authentication attempts (retries) allowable .

Examples

This example shows how to enable the SSH service.

```
Switch# configure terminal
Switch(config)# ip ssh
```

This example shows how to set the SSH timeout to 160 seconds.

```
Switch# configure terminal
Switch(config)# ip ssh timeout 160
```

This example shows how to set the number of SSH authentication-retries to 2. The connection will be failed when the number of authentication retries reaches 2 tries without success.

```
Switch# configure terminal
Switch(config)# ip ssh authentication-retries 2
```

This example shows how to change the service-port to 3000. The SSH client must connect using this service port number.

```
Switch# configure terminal
Switch(config)# ip ssh service-port 3000
```

Verify the settings by entering the **show ip ssh** command.

ip telnet server

Use this command to enable the TELNET server function. Use the no form of the command to disable the TELNET server function.

ip telnet server

no ip telnet server

Syntax None

Default Enabled

Command Mode Global configuration

Usage Guideline Telnet is a network protocol used on the Internet or local area networks to provide a general bidirectional interactive communications facility. Using the Telnet protocol, users can control a device, through a TCP connection which transmits data in plain text.

This command is used to enable/disable the IP TELNET server function. The SSH access interface is separated controlled through SSH commands.

Example This example shows how to enable telnet server function.

```
Switch(config)# ip telnet server
```

Verify the settings by entering the **show system protocol-state** command.

ip telnet service-port

Use this command to specify the service port for the TELNET server. Use the default command to return the service port to 23.

ip telnet service-port *TCP-PORT*

default ip telnet service-port

Syntax Description	
TCP-PORT	The TCP port number. TCP ports are numbered between 1 and 65535. The *well-known* TCP port for the TELNET protocol is 23.

Default TCP-PORT 23

Command Mode Global configuration

Usage Guideline This command configures the TCP port number for the TELNET server. The Telnet server listens on port number 23 for connection requests in the default configuration.

Example This example shows how to change the service port to 3000.

```
Switch(config)# ip telnet service-port 3000
```

Verify the settings by entering the **show system protocol-state** command.

ip trusted-host

Use this command to create the trusted host entries on the switch. Use the **no ip trusted-host** command to remove the trusted host entries.

ip trusted-host {*IP-ADDRESS* | *NETWORK-ADDRESS/PREFIX-LENGTH***} [snmp] [http] [telnet]]**

no ip trusted-host *[IP-ADDRESS | NETWORK-ADDRESS/PREFIX-LENGTH]* **[snmp] [http] [telnet]**

Syntax Description	
IP-ADDRESS	IPv4 address of the trusted host.
NETWORK-ADDRESS/PREFIX-LENGTH	IPv4 network of the trusted host.
snmp	(Optional) Specifies that the host is valid for snmp.
http	(Optional) Specifies that the host is valid for http.
telnet	(Optional) Specifies that the host is valid for telnet.

Default No default hosts

Command Mode Global configuration at privilege level 15.

Usage Guideline The **ip-trusted host** command creates the trusted host entries with access to the management interface. When a trusted-host is not configured, then all hosts are trusted. When adding a trusted-host, if the access interface (snmp, http, or telnet) is not specified, then it applies to all interfaces.

Once a trusted-host is configured with an access interface allowed, then only the configured trusted-hosts are allowed access to the access interfaces associated with their entry. If an access interface is not specified in the trusted-host list, then all access to that access interface will be blocked.

The number of trusted hosts is project dependent.

For the no command, when the host is not specified, all hosts will be deleted for the specified access interface. If no access interface is specified, the specified host will be deleted for all access interfaces. If both the host and access interface are not specified, all trusted hosts will be deleted.

Examples This example shows how to add a trusted host with IP address 163.10.50.126 to snmp access interface.

```
Switch(config)# ip trusted-host 163.10.50.126 snmp
```

This example shows how to remove the trusted host with IP address 163.10.50.126 for all access interfaces.

```
Switch(config)# no ip trusted-host 163.10.50.126
```

You can verify your settings by entering the **show ip trusted-host** command.

ipv6 access-group

Use the **ipv6 access-group** command to specify the IPv6 access-list to be applied to an interface. Use the no form of the command to remove an IPv6 access list.

Ipv6 access-group *NAME* **[in]**

no ipv6 access-group *NAME* **[in]**

Syntax Description	
NAME	The name of the IPv6 access-list to be applied. Up to 32 characters are allowed. The syntax is a general string that does not allow spaces.
in	(Optional) Specifies that the IPv6 access-list will be applied in the **ingress** direction. If no option is specified, the **in** direction is applied.

Default None

Command Mode Interface configuration

Usage Guideline Up to one MAC access-list, one IP access-list and one IPv6 access-list can be applied to the same interface. An error message will be displayed if the user attempts to apply the second IPv6 access list.

The IPv6 access list must be created before it can be applied to the interface. Otherwise, an error message will be displayed.

The keyword **in** specifies the ingress direction check.

The association of an access-group with an interface will consume the filtering entry resource of the switch controller. If the command is applied successfully, the number of remaining maximum entries will be displayed. If the rule of the access-group contains port operator, gt/lt operator, the number of remaining port operators will be displayed. If the resources are insufficient to commit the command, an error message will be displayed.

There is limitation on the number of port operator resources. The maximum number is project dependent.

If the commit, of the command, will exceed the maximum number of available port selectors, an error message will be displayed.

An access-group is applied to the interface, which will consume the filter entry resource. When the access-group is applied successfully, the number of remaining filter entry resource will be displayed. If the access-group were using a port operator (for example: gt/lt) for the rule, it will display the number of remaining port operator resource.

If the remaining resources of filter entry or port operator is insufficient, an error message will display when the access-group is applied.

Example This example shows how to specify the IPv6 access-list ip6-control as an IPv6 access group for eth3.3

```
Switch(config)# interface eth3.3
Switch(config-if)#ipv6 access-group ip6-control in
```

Verify the settings by entering **show access-group**.

ipv6 access-list

Use this command to create or modify an IPv6 access list. This command will enter into the ipv6 access-list configuration mode. Use the no form of the command to remove an IPv6 access-list.

ipv6 access-list extended NAME

no ipv6 access-list extended NAME

Syntax Description	
NAME	The name of the IPv6 access-list to be configured. A maximum of 32 characters. The syntax is a general string that does not allow spaces.

Default

No IPv6 access list is defined.

The access list defaults to an implicit deny statement for all traffic.

Command Mode

Global configuration

Usage Guideline

The name must be unique among all (including MAC, IP, and IPv6) access-lists. The characters are case sensitive.

The maximum number of IPv6 access-list supported by the system is project dependent.

An error message will appear if the allowed number is exceeded after the execution of the command.

An IPv6 access list can not be deleted if it is applied to interfaces.

The access list is always terminated by an implicit deny statement for all traffic.

Examples

This example shows how to configure an IPv6 extended access-list, named ip6-control.

```
Switch(config)#ipv6 access-list extended ip6-control
Swtich(config-ipv6-ext-acl)#permit tcp any 2002:f03::1 ffff::
Switch(config-ipv6-ext-acl)#
```

This example shows how configure an IPv6 extended access-list, named ip6-std-control.

```
Switch(config)#ipv6 access-list extended ip6-std-control
Swtich(config-ipv6-ext-acl)#permit  tcp any fe80::101:1 ffff:ffff:ffff::
Switch(config-ipv6-ext-acl)#
```

Verify the settings by entering the **show access-list** command.

ipv6 address

This command is used to assign the IPv6 address to an interface of the switch. The no form of this command deletes the IPv6 address assigned to the interface.

ipv6 address X:X::X:X/M

no ipv6 address [X:X::X:X/M]

Syntax Description	
X:X::X:X/M	IPv6 network address. This argument must be in the form documented in RFC2373 where the address is specified in hexadecimal format using a 16-bit value between colons. X:X::X:X: IPv6 address M: IPv6 prefix length, maximum length is 64.

Default None

Command Mode VLAN interface configuration

Usage Guideline The VLAN interface must be created first. If IPv6 is disabled, it will be enabled after the IPv6 address is configured. When using the **no ipv6 address** command without other parameters, it removes all ipv6 global addresses configured on this interface.

Example This example shows how to add an IPv6 address to a VLAN interface:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 address 3ffe:501:ffff:0:a01:2ff:fe39:1/64
Switch (config-if) #
```

ipv6 address

This command is used to add or delete an IPv6 address to an interface. The address is configured using an IPv6 general prefix and when set it enables IPv6 processing on the interface. To remove the address from the interface, use the no form of this command.

ipv6 address { I*PV6-ADDRESS/ PREFIX-LENGTH* | *PREFIX-NAME SUB-BITS/ PREFIX-LENGTH* **}**

no ipv6 address { *IPV6-ADDRESS/ PREFIX-LENGTH* | *PREFIX-NAME SUB-BITS/ PREFIX-LENGTH* **}**

Syntax Description	
IPV6-ADDRESS	The IPv6 address to be used.
PREFIX-LENGTH	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. The maximum prefix length can not exceed 64.
PREFIX-NAME	A general prefix, which specifies the leading bits of the network to be configured on the interface. The general prefix name can be 1-16 characters.
SUB-BITS	The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix. **Note**:The general prefix is specified using the *PREFIX-NAME* argument above. The *SUB-BITS* argument must be in the form documented in RFC2373 where the address is specified in hexadecimal using 16-bit values between colons.

Default No IPv6 addresses are assigned to the interface.

Command Mode Interface configuration

Usage Guideline The **ipv6 address** command allows multiple IPv6 addresses to be configured on an interface in a variety of forms with varying options. The most common way is to specify the IPv6 address with the prefix length.

Addresses may also be defined using the general prefix mechanism, which separates the aggregated IPv6 prefix bits from the subprefix and host bits. In this case, the leading bits of the address are defined in a general prefix, which is globally configured or learned (for example, through use of DHCP-PD), and then applied using the prefix-name argument. The subprefix bits and host bits are defined using the sub-bits argument.

Examples

The following example shows how to enable IPv6 processing on the interface and configure an address based on the general prefix called my-prefix and the directly specified bits:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan2
Switch (config-if) # ipv6 address my-prefix 0:0:0:1::1/64
```

Assuming the general prefix named *my-prefix* has the value of 3ffe:1:2::/48, then the interface would be configured with the global address: 3ffe:1:2:1::1/64. If no general prefix named *my-prefix* is set, then no IPv6 address will be set.

If the general prefix named my-prefix is an acquired through a DHCPv6 Client prefix delegation, then the global address would be configured after the prefix is received from the DHCPv6 Client.

The following example shows how to remove a general prefix named *my-prefix* on the interface:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan2
Switch (config-if) # no ipv6 address my-prefix 0:0:0:1::1/64
```

The following example shows how to manually configure a global address:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan2
Switch (config-if) # ipv6 address 3ffe:22:22:22::2/64
```

After the command is entered, the global address 3ffe:22:22:22::2/64 will be immediately set.

The following example shows how to manually remove a global address from the configuration:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan2
Switch (config-if) # no ipv6 address 3ffe:22:22:22::2/64
```

After the command is entered, the global address 3ffe:22:22:22::2/64 will be immediately removed.

ipv6 address (management port)

Use this command to set the IPv6 address of the Management Port. Use the no form of this command to set the IPv6 address of the Management Port to the default value.

ipv6 address *IPv6-ADDRESS/PREFIX-LENGTH*

no ipv6 address

Syntax Description	
IPv6-ADDRESS	IPv6 address, X:X::X:X
PREFIX-LENGTH	Prefix Length.

Default Default IPv6 address is: **::/0**.

Command Mode Management interface configuration

Usage Guideline Users can manage the system by accessing this IPv6 address. Use the **no ipv6 address** command to restore the default IPv6 address

Example This example shows how to set 2000::1/64 as the IPv6 address of the Management Port.

```
Switch(mgmt-if)#
Switch(mgmt-if)#ipv6 address 2000::1/64
```

Verify the settings by entering the **show mgmt-if** command

ipv6 default-gateway (management port)

Use this command to set the IPv6 address of the IPv6 default gateway that is used by the management port. Use the no form of this command to set the IPv6 default gateway to the default value.

ipv6 default-gateway *IPv6-ADDRESS*

no ipv6 default-gateway

Syntax Description	
IPv6-ADDRESS	IPv6 address, X:X::X:X

Default ::

Command Mode Management interface configuration

Usage Guideline The management port will send out IPv6 packets destined for other IP subnets using this IPv6 address as the gateway router.

Example This example shows how to set 2000::2 as the IPv6 address of the default gateway.

```
Switch(mgmt-if)#ipv6 default-gateway 2000::2
Switch(mgmt-if)#
```

Verify the settings by entering the **show mgmt-if** command

ipv6 dhcp client information refresh minimum

To configure the minimum acceptable refresh time of the DHCPv6 client information on a specified interface. To remove the configured refresh time, use the no form of this command.

ipv6 dhcp client information refresh minimum *SECONDS*

no ipv6 dhcp client information refresh minimum

Syntax Description	
SECONDS	The refresh time, in seconds. The minimum value that can be used is 600 seconds, and the maximum value can be 65535 seconds.

Default Unlimited

Command Mode Interface configuration

Usage Guideline The **ipv6 dhcp client information refresh minimum** command specifies the minimum acceptable refresh time of the DHCPv6 client information. If the server sends an information refresh time option of less than the configured minimum refresh time, the configured minimum refresh time will be used instead.

This command may be configured in several situations:

- In unstable environments where unexpected changes are likely to occur.
- For planned changes, including renumbering, an administrator can gradually decrease the time as the planned event nears.
- Limit the amount of time before new services or servers are available to the client, such as the addition of a new Simple Network Time Protocol (SNTP) server or a change of address for a Domain Name System (DNS) server.

Setting **ipv6 dhcp client information refresh minimum** or **no ipv6 dhcp client information refresh minimum** will not enable or disable the DHCPv6 client prefix delegation function.

Example The following example configures a maximum of 2 hours before the DHCPv6 client information will be refreshed:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 dhcp client information refresh minimum 7200
```

ipv6 dhcp client pd

This command enables a specified IPv6 interface's DHCP client process and it enables the request for prefix delegation through the same interface. To disable requests for prefix delegation, use the no form of this command.

ipv6 dhcp client pd { *PREFIX-NAME* **| hint** *IPV6-PREFIX* **} [rapid-commit]**

no ipv6 dhcp client pd

Syntax Description	
PREFIX-NAME	IPv6 general prefix name. The prefix name will be associated with general prefix-name setting of an interface. The general prefix name can be 1-16 characters.
hint	An IPv6 prefix sent as a hint.
IPV6-PREFIX	IPv6 general prefix. It will be filled in the Solicit message to request an IPv6 prefix.
rapid-commit	(Optional) Allow two-message exchange method for prefix delegation. The rapid-commit option will be filled in the Solicit message to request two message handshaking.

Default The prefix delegation is disabled.

Command Mode Interface configuration

Usage Guideline If DHCPv6 is not running yet, executing the ipv6 dhcp client pd command starts the DHCPv6 protocol for an IPv6 client process. Use **no ipv6 dhcp client pd** to disable the DHCPv6 client.

Further, the **ipv6 dhcp client pd** command enables r*equest for prefix delegation* on the interface where this command is configured. When prefix delegation is enabled and a prefix is successfully acquired, the prefix is stored in the IPv6 general prefix pool with an internal name defined by the IPV6-PREFIX argument. Other commands and applications (such as the **ipv6 address** command) can then refer to the prefixes in the general prefix pool.

The hint keyword with the IPV6-PREFIX argument enables the configuration of an IPv6 prefix. That prefix will be included in DHCHv6 solicit and request messages sent by the interface's IPv6 client DHCP. The included prefixes, in the messages, are sent as a hint for the prefix-delegating routers. Only one prefix can be configured for each delegation hint request message.

Re-configuring prefix hint will change the hint setting, and setting **no ipv6 dhcp client pd** will clear the prefix hint option. Care should be taken in setting the hint option as it will not enable DHCPv6 client prefix delegation function.

The rapid-commit keyword enables the use of the two-message exchange protocol for prefix delegation and other settings. If it is enabled, the client will include the rapid commit option in a solicit message.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface.

Examples

The following example enables prefix delegation, where dhcp-prefix is the genenal prefix name configured by ipv6 address command.

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan2
Switch (config-if) # ipv6 address dhcp-prefix 0:0:0:7272::72/64
Switch (config-if) # exit
Switch (config) # interface vlan1
Switch (config-if) # ipv6 dhcp client pd dhcp-prefix
```

The following example configures a hint for prefix-delegation.

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 dhcp client pd hint 2001:0DB8:1::/48
```

The following example configures a rapid-commit delegation.

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 dhcp client pd dhcp-prefix rapid-commit
```

The following example configures a delegation with hint prefix and rapid-commit simultaneously.

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 dhcp client pd hint 2001:0DB8:1::/48
Switch (config-if) # ipv6 dhcp client pd dhcp-prefix rapid-commit
```

ipv6 dhcp relay destination

These commands are used to enable or disable the DHCP relay function.

ipv6 dhcp relay destination *IPV6-ADDRESS [VLAN-INTERFACE*]

no ipv6 dhcp relay destination

Syntax Description	
IPV6-ADDRESS	Relay destination address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
VLAN-INTERFACE	Relay to which VLAN-interface. Valn-interface specifies output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.

Default DHCP relay: Disabled

IPV6-ADDRESS: None

VLAN-INTERFACE: NULL.

Command Mode Interface configuration

Usage Guideline The **ipv6 dhcp relay destination** command specifies a destination address to which client messages are forwarded and it enables DHCP for IPv6 relay service on the interface. When relay service is enabled on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations. The incoming DHCP for IPv6 message may have come from a client on that interface, or it may have been relayed by another relay agent.

The relay destination can be a unicast address of a server or another relay agent, or it may be a multicast address. The following are the two types of relay destination addresses:

- A link-scoped unicast or multicast IPv6 address, for which, a user must specify an output interface
- A global or site-scoped unicast or multicast IPv6 address, for which, a user CANNOT specify the output interface. The output interface will determined by routing table.

If no output interface is configured for a destination, the output interface is determined by routing tables. In this case, it is recommended that a unicast or multicast routing protocol be running on the router. Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays messages to a multicast address, it sets the hop limit field in the IPv6 packet header to 32.

Unspecified, loopback and node-local multicast addresses are not acceptable as the relay destination. If any one of them is configured, the message "Invalid destination address" is displayed.

Note that it is not necessary to enable the relay function on an interface for it to accept and forward an incoming relay reply message from servers. By default, the relay function is disabled, and there is no relay destination on an interface. The no form of the command removes a relay destination on an interface or deletes an output interface for a destination. If all relay destinations are removed, the relay service is disabled on the interface.

DHCP for the IPv6 client, server, and relay functions is mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: "Interface is in DHCP client mode," "Interface is in DHCP server mode," or "Interface is in DHCP relay mode."

One VLAN interface only can be configured to one DHCP relay server.

Example

This example shows how to sets the relay destination server address on vlan1:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056
vlan2
```

This example shows how to disable relay agent on vlan1

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # no ipv6 dhcp relay destination
```

ipv6 enable

This command is used to enable and disable the IPv6 protocol on an interface of the switch. The no form of this command can disable the IPv6 protocol.

ipv6 enable

no ipv6 enable

Syntax None

Default The default IPv6 incidence status is "Disable".

Command Mode The VLAN interface must be created before.

Usage Guideline The interface must be created before used ipv6 enable command. When the interface up, **ipv6 enable** will also add link-local address to the interface and vice versa. When global address had existed in the interface and using the "**no ipv6 enable**" command, it will take no effect (link-local address should not be removed).

Example This example shows how to enable the IPv6 protocol:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 enable
Switch (config-if) #
```

ipv6 hop-limit

This command is used to configure the IPv6 hop limit setting for an interface of this switch. The no form of this command resets the IPv6 hop limit to the default value.

ipv6 hop-limit *<0-255>*

no ipv6 hop-limit

Syntax Description	
<0-255>	The IPv6 hop limit range, "0" means not specified on this interface and to use the default value to send a packet.

Default Hop limit: 64

Command Mode VLAN interface configuration

Usage Guideline The VLAN interface must be created first before this command can be used.

Example This example shows how to configure IPv6 hop limit setting:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 hop-limit 255
Switch (config-if) #
```

ipv6 nd managed-config-flag

This command is used to turn on the IPv6 RA (router advertisement) management configure flag setting on an interface of this switch. The no form of this command turns off this flag.

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Syntax None

Default Off

Command Mode VLAN interface configuration

Usage Guideline The VLAN interface must be created first before this command can be used.

Example This example shows how to configure IPv6 manage config flag setting:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 nd managed-config-flag
Switch (config-if) #
```

ipv6 nd other-config-flag

This command is used to turn on the IPv6 RA (router advertisement) other configure flag incidence per interface on this switch. The no form of this command turns off this flag.

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Syntax None

Default **other configure flag**: off

Command Mode VLAN interface configuration

Usage Guideline The VLAN interface must be created first before this command can be used.

Example This example shows how to configure IPv6 other configure flag incidence:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 nd other-config-flag
Switch (config-if) #
```

ipv6 nd prefix

This command is used to add or modify IPv6 prefix information to RA (router advertisement) for an interface of this switch. If the prefix already exists, then the command modifies the parameter. The no form of the command removes it.

ipv6 nd prefix X:X::X:X/M *<0-4294967295>* *<0-4294967295>* **[off-link | no-autoconfig]**

no ipv6 nd prefix X:X::X:X/M

Syntax Description	
X:X::X:X/M	IPv6 network address. This argument must be in the form documented in RFC2373 where the address is specified in hexadecimal format using a 16-bit value between colons. X:X::X:X: IPv6 address M: IPv6 prefix length
<0-4294967295>	Valid life time in seconds.
<0-4294967295>	Preferred lifetime in seconds.
off-link	Turn off on-link flag.
no-autoconfig	Turn off autoconfig flag.

Default

0-4294967295: 2592000

0-4294967295: 604800

off-link: On

no-autoconfig: On

Command Mode

VLAN interface configuration

Usage Guideline

The VLAN interface must be created first before this command can be used.

Example

This example shows how to configure IPv6 prefix information incidence:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 nd prefix 3ffe:501:ffff:100::/64 30000 20000
Switch (config-if) #
```

ipv6 nd ra-interval

This command is used to configure the IPv6 RA (router advertisement) interval timer for an interface of this switch. The no form of this command sets the lifetime to the default value.

ipv6 nd ra-interval *<4-1800> [<3-1350>]*

no ipv6 nd ra-interval

Syntax Description	
<4-1800>	Maximum interval value in seconds.
<3-1350>	Minimum interval value in seconds. Must be smaller than the maximaum value * 0.75

Default *<4-1800>: 600*

<3-1350>: 198

Command Mode VLAN interface configuration

Usage Guideline The VLAN interface must be created first before this command can be used. If the minimum interval value is not configured, the minimum interval value will be automatically assigned per the following rules.

1.If maximum timer >= 9 seconds, then it is configured to the maximum value * 0.33.

2.If maximum timer < 9 seconds, then it is configured to the maximum value.

Example This example shows how to configure the IPv6 RA interval timer setting:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 nd ra-interval 1500 1000
Switch (config-if) #
```

ipv6 nd ra-lifetime

This command is used to configure the IPv6 RA (router advertisement) lifetime on an interface of this switch. The no form of this command sets the lifetime to the default value.

ipv6 nd ra-lifetime <*0-9000*>

no ipv6 nd ra-lifetime

Syntax Description	
<0-9000>	The IPv6 router advertisement lifetime range in seconds.

Default 1800

Command Mode VLAN interface configuration

Usage Guideline The VLAN interface must be created first before this command can be used.

Example This example shows how to configure IPv6 ra lifetime incidence:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 nd ra-lifetime 9000
Switch (config-if) #
```

ipv6 nd reachable-time

This command is used to configure IPv6 RA (router advertisement) reachable time on an interface of this switch. The no form of this command sets the reachable time to the default value.

ipv6 nd reachable-time *<0-3600000>*

no ipv6 nd reachable-time

Syntax Description	
<0-3600000>	The IPv6 router advertisement reachable time range in milliseconds.

Default 0

Command Mode VLAN interface configuration

Usage Guideline The VLAN interface must be created first before this command can be used. When the reachable time is set to the default value or set to "0", the system will run for 30 seconds on this interface, but the RA packet will be set to "0".

Example This example shows how to configure the IPv6 reachable time setting:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 nd reachable time 3600000
Switch (config-if) #
```

ipv6 nd retrans-timer

This command is used to configure IPv6 RA (router advertisement) retrans timer per interface on this switch. The no form of this command sets the retrans timer to the default value.

ipv6 nd retrans-timer <*0-4294967295***>**

no ipv6 nd retrans-timer

Syntax Description	
<0-4294967295>	The IPv6 router advertisement retrans timer range in milliseconds.

Default 0

Command Mode VLAN interface configuration

Usage Guideline The VLAN interface must be created first before this command can be used. When the reachable time is set to the default value or set to "0", the system will use 1 second for this interface, but the RA packet will be set to "0".

Example This example shows how to configure the IPv6 retrans timer setting:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 nd retrans-timer 4294967295
Switch (config-if) #
```

ipv6 nd suppress-ra

This command is used to suppress IPv6 RA (router advertisement) on an interface of this switch. Use the **no ipv6 nd suppress-r**a configuration command to enable the sending of IPv6 router advertisements on an ISATAP tunnel interface.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Syntax None

Default Suppress RA

(Sending of IPv6 router advertisements is disabled by default on an ISATAP tunnel interface)

Command Mode VLAN interface configuration

Usage Guideline The VLAN interface must be created first before this command can be used.

ISATAP tunnel interfaces are valid for this command. Other types of tunnel interfaces are invalid.

Example This example shows how to suppress IPv6 RA's:

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if) # ipv6 nd suppress-ra
```

ipv6 neighbor

This command is used to add a static ipv6 neighbor entry. The no form of this command deletes the IPv6 neighbor entry.

ipv6 neighbor X:X::X:X IFNAME MAC

no ipv6 neighbor X:X::X:X IFNAME

Syntax Description	
X:X::X:X	IPv6 address. This argument must be in the form documented by RFC2373 where the address is specified in hexadecimal using a 16-bit value between colons. XXXX: IPv6 address
IFNAME	The IP Interface name
MAC	The MAC address, in XX-XX-XX-XX-XX-XX format

Default None

Command Mode Global configuration.

Usage Guideline None

Example This example shows how to configure an IPv6 neighbor entry:

```
Switch > enable
Switch # configure terminal
Switch (config) # ipv6 neighbor fe80::1 vlan1 00-01-80-11-22-99
Switch (config) #
```

ipv6 ospf cost

To explicitly specify the cost of sending a packet on an interface, use the **ipv6 ospf cost command**. To reset the interface cost to the default value, use the no form of this command.

ipv6 ospf cost *COST* **[instance-id** *INSTANCE-ID***]**

no ipv6 ospf cost [instance-id *INSTANCE-ID***]**

Syntax Description	
COST	Unsigned integer value expressed as the link-state metric. It can be a value in the range from 1 to 65535.
INSTANCE-ID	(Optional) Instance identifier. To change this ID, please issue the "no" command first. The valid setting is from 0 to 255.

Default *Cost*: Unconfigured

INSTANCE-ID: 0

Command Mode Interface configuration

Usage Guideline To modify the cost from the default value, set the metric manually using the **ipv6 ospf cost** command. Using the **bandwidth** command changes the link cost as long as the **ipv6 ospf cos**t command is not used. The link-state metric is advertised as the link cost in the router link advertisement.

Example The following example sets the interface cost value to 65.

```
Switch > enable
Switch # configure terminal
Switch (config)# interface vlan1
Switch (config-if)# ipv6 ospf cost 65
```

ipv6 ospf dead-interval

To set the time period used, during which hello packets are not detected, before neighbors declare the router down, use the **ipv6 ospf dead-interval** command. To return to the default time, use the no form of this command.

ipv6 ospf dead-interval *SECONDS* **[instance-id** *INSTANCE-ID***]**

no ipv6 ospf dead-interval [instance-id *INSTANCE-ID***]**

Syntax Description	
SECONDS	Specifies the interval in seconds. The value must be the same for all nodes on a specific network.It can be a value in the range from 1 to 65535.
INSTANCE-ID	(Optional) Instance identifier. To change this ID, please configure "no" command first. The valid setting is from 0 to 255.

Default *Seconds*: 40

Default INSTANCE-ID: 0

Command Mode Interface configuration

Usage Guideline The interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network.

Example The following example sets the IPv6 OSPF dead interval to 60 seconds.

```
Switch > enable
Switch # configure terminal
Switch (config)# interface vlan1
Switch (config-if)# ipv6 ospf dead-interval 60
```

ipv6 ospf hello-interval

To specify the interval between hello packets sent from an interface, use the **ipv6 ospf hello-interval** command. To return to the default time, use the no form of this command.

ipv6 ospf hello-interval *SECONDS* **[instance-id** *INSTANCE-ID***]**

no ipv6 ospf hello-interval [instance-id *INSTANCE-ID***]**

Syntax Description	
SECONDS	Specifies the interval in seconds. The value must be the same for all nodes on a specific network. It can be a value in the range from 1 to 65535.
INSTANCE-ID	(Optional) Instance identifier. To change this ID, configure the "no" command first. The valid setting is from 0 to 255.

Default *Seconds*: 10

INSTANCE-ID: 0

Command Mode Interface configuration

Usage Guideline This value is advertised in the hello packets. The shorter the hello interval, the earlier topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Example The following example sets the interval between hello packest to 15 seconds.

```
Switch > enable
Switch # configure terminal
Switch (config)# interface vlan1
Switch (config-if)# ipv6 ospf hello-interval 15
```

ipv6 ospf priority

To set the router priority, which helps determine the designated router for this network, use the **ipv6 ospf priority**. To return to the default value, use the no form of this command.

ipv6 ospf priority *PRIORITY* **[instance-id** *INSTANCE-ID***]**

no ipv6 ospf priority [instance-id *INSTANCE-ID***]**

Syntax Description	
PRIORITY	A number value that specifies the priority of the router. The range is from 0 to 255.
INSTANCE-ID	(Optional) Instance identifier.To change this ID, please configure "no" command first.The valid setting is from 0 to 255.

Default *Priority*: 1

INSTANCE-ID: 0

Command Mode Interface configuration

Usage Guideline Seting the priority helps determine the OSPF Designated Router (DR) for a network. If two routers attempt to become the DR, the router with the higher router priority becomes the DR. If the router priority is the same for two routers, the router with the higher router ID takes precedence.

Only routers with non-zero router priority values are eligible to become the designated or backup designated router. Configure router priority for multi-access networks (not point-to-point) only.

Example The following example sets the router priority value to 4.

```
Switch > enable
Switch # configure terminal
Switch (config)# interface vlan1
Switch (config-if)# ipv6 ospf priority 4
```

ipv6 ospf retransmit-interval

This command specifies the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to an interface.

ipv6 ospf retransmit-interval *SECONDS* **[instance-id** *INSTANCE-ID***]**

no ipv6 ospf retransmit-interval [instance-id *INSTANCE-ID***]**

Syntax Description	
SECONDS	The interval the router waits before it retransmits a packet. The valid setting is 1-65535.
INSTANCE-ID	(Optional) Instance identifier. In order to change this ID, configure the "no" command first. The valid setting is from 0 to 255.

Default *Seconds:* 5

INSTANCE-ID: 0

Command Mode Interface configuration

Usage Guideline After sending an LSA to a neighbor, the router keeps the LSA until it receives an acknowledgement. In case the router does not receive an acknowledgement, during the set time (the retransmit interval value), it retransmits the LSA. Set the retransmission interval value conservatively to avoid needless retransmissions. The interval should be greater than the expected round-trip delay between two routers.

Example The following example sets the retransmit interval value to 6 seconds.

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if)# ipv6 ospf retransmit-interval 6
```

ipv6 ospf shutdown

To initiate an IPv6 OSPF protocol graceful shutdown at the interface level, use the **ipv6 ospf shutdown** command. To restart the OSPF protocol on an interface, use the no form of this command

ipv6 ospf shutdown [*IFNAME***]**

no ipv6 ospf shutdown [*IFNAME***]**

Syntax Description	
IFNAME	(Optional) Interface type and number. If no option is specified, apply to the whole IPv6 OSPF process.

Default Disabled

Command Mode Router configuration

Usage Guideline Use the **ipv6 ospf shutdown** command to put IPv6 OSPF under a specific interface in shutdown mode. If no interface is specified for this command in router configuration mode, it will shutdown the protocol in the least disruptive manner and notify its neighbors that it is leaving. All traffic, that has another path through the network, will be directed to that alternate path.

Note: When this command is used to shutdown IPv6 OSPF on all interfaces, then at this time the device will clear the LSDBs and leave them empty. This behavior is not the same as with the IPv4 OSPF protocol.

Example The following example shows how to initiate an IPv6 OSPF protocol shutdown on the layer 3 interface (VLAN 1):

```
Switch > enable
Switch # configure terminal
Switch (config) # router ipv6 ospf
Switch (config-router)# ipv6 ospf shutdown vlan1
```

ipv6 ospf transmit delay

To set the estimated time required to send a link-state update packet on the interface, use the **ipv6 ospf transmit-delay** command. To return to the default value, use the no form of this command.

ipv6 ospf transmit-delay *SECONDS* **[instance-id** *INSTANCE-ID***]**

no ipv6 ospf transmit-delay [instance-id *INSTANCE-ID]*

Syntax Description	
SECONDS	The interval the router waits before it transmits a packet. The valid setting is 1-65535.
INSTANCE-ID	(Optional) Instance identifier. To change this ID, configure the "no" command first. The valid setting is from 0 to 255.

Default *SECONDS*: 1

INSTANCE-ID: 0

Command Mode Interface configuration

Usage Guideline Before being transmited, Link-State Advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the seconds. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which LSAs propagate over the link will not be considered. This setting has more significance on very low-speed links.

Example The following example sets the transmit delay value to 3 seconds.

```
Switch > enable
Switch # configure terminal
Switch (config) # interface vlan1
Switch (config-if)# ipv6 ospf transmit-delay 3
```

ipv6 rip metric-offset

To set the IPv6 RIP metric for an interface, use the **ipv6 rip metric-offse**t command. To return the metric to its default value, use the no form of this command.

ipv6 rip metric-offset *METRIC-VALUE*

no ipv6 rip metric-offset

Syntax Description	
METRIC-VALUE	Value added to the metric of an IPv6 RIP route received in a report message. A number from 1 to 16.

Default The default metric value is 1.

Command Mode Interface configuration

Usage Guideline When an IPv6 RIP route is received, the interface metric value set by the **ipv6 rip metric-offset** command is added before the route is inserted into the routing table. Increasing the IPv6 RIP metric value of an interface will increase the metric value of IPv6 RIP routes received over the interface.

Use the **ipv6 rip metric-offset** command to influence which routes are used.

The IPv6 RIP metric is in the hop count.

Example The following example configures a metric increment of 10 for the RIP routing process.

```
Switch > enable
Switch # configure terminal
Switch (config)# interface vlan1
Switch (config-if)# ipv6 rip metric-offset 10
```

ipv6 rip split-horizon

To enable IPv6 RIP split-horizon mechanism, use the **ipv6 rip split-horizon** command. To disable the split horizon processing of IPv6 RIP updates, use the no form of this command.

ipv6 rip split-horizon

no ipv6 rip split-horizon

Syntax None

Default This command is disabled by default.

Command Mode Interface configuration

Usage Guideline This command configures split horizon processing of IPv6 RIP router updates. If split horizon is configured on interfaces where the networks are learned, then the advertisement of networks sent out from those same interfaces is suppressed.

When both split horizon and poison reverse are configured, then split horizon behavior is replaced by poison reverse behavior routes. The poison reverse behavior routes are learned via RIP and are advertised out the interface over which they were learned. They are advertised with an unreachable metric.

Example The following example configures split horizon processing for the IPv6 RIP routing process.

```
Switch > enable
Switch # configure terminal
Switch (config)# interface vlan1
Switch (config-if)# ipv6 rip split-horizon
```

ipv6 rip split-horizon poisoned

To configure the poison reverse processing of IPv6 RIP router updates, use the **ipv6 rip split-horizon poisoned** command. To disable the poison reverse processing of IPv6 RIP updates, use the no form of this command.

ipv6 rip split-horizon poisoned

no ipv6 rip split-horizon

Syntax None

Default Poison reverse is configured.

Command Mode Interface configuration

Usage Guideline This command configures poison reverse processing of IPv6 RIP router updates. When poison reverse is configured, routes learned via RIP are advertised with an unreachable metric out from the interface over which they were learned.

If both poison reverse and split horizon are configured, then simple split horizon behavior is replaced by poison reverse behavior.

Example The following example configures poison reverse processing for the IPv6 RIP routing process.

```
Switch > enable
Switch # configure terminal
Switch (config)# interface vlan1
Switch (config-if)# ipv6 rip split-horizon poisoned
```

ipv6 ospf mtu-ignore

To disable IPv6 Open Shortest Path First (OSPF) maximum transmission unit (MTU) mismatch detection on receiving database descriptor (DBD) packets, use the ipv6 ospf mtu-ignore command in interface configuration mode. To reset to default, use the no form of this command.

ipv6 ospf mtu-ignore [instance-id *INSTANCE-ID***]**

no ipv6 ospf mtu-ignore [instance-id *INSTANCE-ID***]**

Syntax Description	
INSTANCE-ID	(Optional) Instance identifier. If you want to change this ID, please configure "**no**" command first. The range is from 0 to 255.

Default IPv6 OSPF MTU mismatch detection is enabled.

Command Mode Interface configuration mode

Usage Guideline IPv6 OSPF checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher than the IP MTU configured on the incoming interface, IPv6 OSPF adjacency will not be established.

Example The following example disables MTU mismatch detection on receiving DBD packets..

```
Switch > enable
Switch # configure terminal
Switch (config)# interface vlan1
Switch (config-if)# ipv6 ospf mtu-ignore
```

ipv6 route

Use **ipv6 route** to add an IPv6 static route entry. Use the no form of the command to remove an IPv6 static route entry.

ipv6 route *NETWORK-PREFIX* / *PREFIX-LENGTH* {*NEXT-HOP-ADDRESS* | *INTERFACE-TYPE INTERFACE-NUMBER NEXT-HOP-ADDRESS*} **[distance** *DISTANCE***]**

no ipv6 route *NETWORK-PREFIX / PREFIX-LENGTH* [*NEXT-HOP-ADDRESS* | *INTERFACE-TYPE* I*NTERFACE-NUMBER NEXT-HOP-ADDRESS*]

Syntax Description	
NETWORK-PREFIX / PREFIX-LENGTH	The network prefix and the prefix length specify the destination network.
NEXT-HOP-ADDRESS	The IPv6 address of the next hop that can be used to reach the specified network. **Note**: An interface must be specified when using a link-local address as the next hop (the link-local next hop must also be an adjacent router). If an interface is specified, a global IPv6 address cannot be used as the next hop address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
INTERFACE-TYPE	Interface type. For more information about supported interface types, use the question mark (?) online help function. When using the interface-type argument with tunnel interfaces, there is no need to specify the *NEXT-HOP-ADDRESS.* When using the interface-type argument with broadcast interfaces, always specify the *NEXT-HOP-ADDRESS* or ensure that the specified prefix is assigned to the link. A link-local address should be specified as the next hop for broadcast interfaces.
INTERFACE-NUMBER	Interface number. For more information about the numbering syntax for supported interface types, use the question mark (?) online help function.
DISTANCE	(Optional) An administrative distance. The default value is 1, which gives static routes precedence over any other type of route except connected routes.

Default No static route is configured.

Command Mode Global configuration

Usage Guideline: See the following sections.

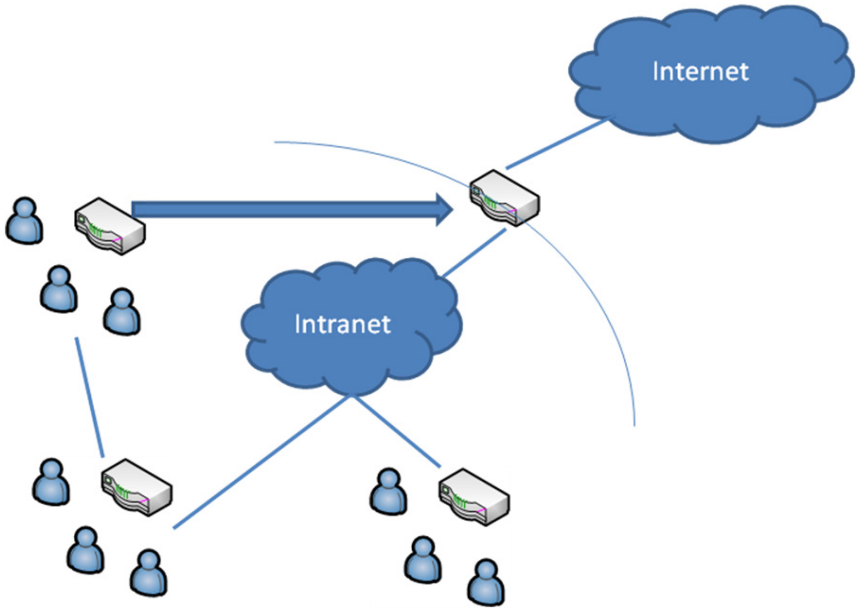
Configuring Default Route Configuring a default route is useful and simple for managing the IPv6 forwarding path. By giving the NETWORK-PREFIX and PREFIX-LENGTH as zero, the system will setup the default path(s) for IPv6 traffic. Using the following commands to create or delete the default route of the system.

Practical Usage

Operators may prefer to specify a default path for the managed devices. By specifying a default gateway, traffic inside the managed topology always has the proper path to follow. Usually, routers on smaller networks may need this configuration, since they have less CPU computing power or less memory to keep the entire routing table of the topology.

Examples

Imagine the topology is illustrated below. The device on the edge may not have enough power to forward all the IPv6 traffic to the world. Therefore, it needs a default route to serve the connected IPv6 nodes to communicate with nodes on Internet.



This example shows how to create a default route.

```
Switch > enable
Switch # configure terminal
Switch (config) # ipv6 route ::/0 vlan 1 fe80::0200:00ff:fe00:a0a0
```

After configuring the default route, the edge router will forward the unknown IPv6 traffic to the core router. By doing this, users connected to the edge router can connect to the world (WAN/internet).

This example shows how to delete an existing default route.

```
Switch > enable
Switch # configure terminal
Switch (config) # no ipv6 route ::/0 vlan 1 fe80::0200:00ff:fe00:a0a0
```

Configuring a General Static Route

To establish static IPv6 routes, use the **ipv6 route** command in global configuration mode. To remove a previously configured static route, use the no form of this command.

Default

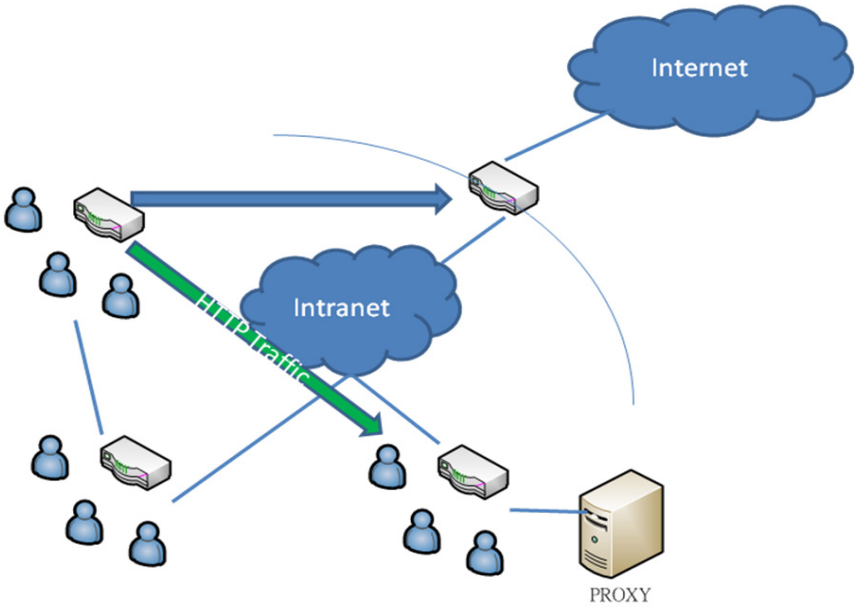
No static routes are configured.

Practical Usage

Operators may prefer to specify the forwarding path of certain traffic. By doing this, the traffic of certain applications in the managed domain will always be forwarded to the expected destination. When the network prefixes and prefix-length are both zero, it implies the specific static route is the default route. A default route presents the final forwarding path of choice should the system not find the matched forwarding rule in routing table. By assigning the address of the next-hop only, the system will forward the IP traffic to this address if, there is no matched forwarding rule by default.

Examples

Imagine the topology as illustrated below. There is a proxy server to access the Intranet. All the users on the Intranet are required to setup this same proxy to communicate with the WEB servers outside the Intranet. However, there is a default gateway configured on the edge route. The HTTP communication from users connected to the edge router will exhaust all the bandwidth available for the Intranet. Therefore, we need a static route to save the bandwidth available for the Intranet.



This example shows how to create a static route destined for the network where proxy server resides.

```
Switch > enable
Switch # configure terminal
Switch (config) # ipv6 route 2001:0DB8::/32 vlan 1 fe80::0200:00ff:fe00:a0a0
```

Then we can use the show command to check whether the configured static route works or not.

```
Switch > enable
Switch # show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - IS-IS, B - BGP

C   2177:0:4:141::/64 is directly connected, vlan141
S   2177:0:3:134::/64 [1/0] via 2177:0:4:906::8003

Total Entries: 2 entries, 2 routes
```

This example shows how to delete an existing static route.

```
Switch > enable
Switch # configure terminal
Switch (config) # no ipv6 route 2001:0DB8::/32 vlan 1
fe80::0200:00ff:fe00:a0a0
```

Configuring a Floating Static Route

Usually, floating static routes are static routes that are being used to back up dynamic routes learned through configured routing protocols. Normally a floating static route is configured with a higher administrative distance than the dynamic routing protocol it is backing up. As a result, the dynamic route learned through the routing protocol is always used in preference to the floating static route. If the dynamic route learned through the routing protocol is lost, the floating static route will be used in its place. That is an IPv6 floating static route can be achieved through the ipv6 route command with a greater distance number. Additionally, to extend the usability, floating static routes can also be allowed to back up static routes, since each route in a system has its own distance.

To establish floating static IPv6 routes, use the **ipv6 route** command in global configuration mode. To remove a previously configured floating static route, use the no form of this command.

Default

No floating static routes are configured.

Practical Usage

Operators may like to specify the priorities of multiple routes destined for the same network. When multiple routes destined for the same network exist, a network device needs to decide which route should be registered into the routing table. The higher priority routes will be active, while lower priority routes will be backup. The following lists the default priority of available kinds of routes in the system.

- LOCAL INTERFACE 0
- STATIC 1

- RIP 120
- RIPNG 120
- OSPF 110
- OSPF6 110
- EBGP 20
- IBGP 200
- ISIS 115

Examples

Assume that a routing protocol originates the same route to the same destination as an existing static route. However, an operator would like to select the calculation of the best route to choose from the routing protocols first. To do that the operator needs to change the priority of the static route, since the default priority of static routes is usually higher than dynamic routes.

This example shows how to create floating static routes. The System will ultimately choose the higher priority (with less distance value) route to be the master route toward the same destination. In this case, the route with distance 11 will be chosen as the master route toward the destination 2001:0DB8::/32.

```
Switch > enable
Switch # configure terminal
Switch (config) # ipv6 route 2001:0DB8::/32 vlan 1 fe80::0200:00ff:fe00:a0a0
distance 11
Switch (config) # ipv6 route 2001:0DB8::/32 vlan 2 fe80::0200:00ff:fe00:b0b0
distance 22
```

This example shows how to delete the previously configured static route.

```
Switch > enable
Switch # configure terminal
Switch (config) # no ipv6 route 2001:0DB8::/32 vlan 1
fe80::0200:00ff:fe00:a0a0
```

ipv6 router ospf area

To enable IPv6 OSPF on an interface, use the **ipv6 router ospf area** command. To disable IPv6 OSPF routing for interfaces defined, use the no form of this command.

ipv6 router ospf area *AREA-ID* **[tag** *PROCESS-ID***] [instance-id** *INSTANCE-ID***]**

no ipv6 router ospf area *AREA-ID* **[tag** *PROCESS-ID***] [instance-id** *INSTANCE-ID***]**

Syntax Description	
AREA-ID	The identifier of the area for which the vlan interface is to be enabled. It can be specified as either a decimal value or as an IPv4 address.
PROCESS-ID	(Optional) An internally used identification parameter for an IPv6 OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each IPv6 OSPF routing process.
INSTANCE-ID	(Optional) Instance identifier. To change this ID, configure the "no" command first. The valid setting is from 0 to 255.

Default IPv6 OSPF is disabled.

PROCESS-ID: null

INSTANCE-ID: 0

Command Mode Interface configuration

Usage Guideline Before enabling IPv6 OSPF on an interface using the **ipv6 router ospf area** command, IPv6 must be enabled on the interface, and IPv6 routing must be enabled on the switch. There is no limit to the number of **ipv6 router ospf area** commands that can be used on the router. At least two interfaces must be configured for IPv6 OSPF to run.

If the configuration is based on a specific process, then the no form of the command must include the process information.

Example The following example enables IPv6 OSPF on an interface.

```
Switch > enable
Switch # configure terminal
Switch (config)# interface vlan1
Switch (config-if)# ipv6 router ospf area 0 instance-id 2
```

ipv6 router rip

To enable the IPv6 RIP routing process on an interface, use the **ipv6 router rip** command. To disable the IPv6 RIP routing process on an interface, use the no form of this command.

ipv6 router rip

no ipv6 router rip

Syntax None

Default Disabled

Command Mode Interface configuration

Usage Guideline The **ipv6 router rip** interface configuration command is used to enable IPv6 RIP explicitly on required interfaces. In IPv4, the **network network-numbe**r router configuration command is used to implicitly specify the interfaces on which to run IPv4 RIP.

Example The following example enables the IPv6 RIP routing process on VLAN 1.

```
Switch > enable
Switch # configure terminal
Switch (config)# interface vlan1
Switch (config-if)# ipv6 router rip
```

key

Use the **key** command to identify a key on a key chain used for routing protocol authentication. Use the **no key** command to remove the key from the key chain.

key *KEY-ID*

no key *KEY-ID*

Syntax Description	
KEY-ID	The iIdentification number of an authentication key of a key chain. The available range for the key ID is a number from 0 to 2147483647, up to 32 key IDs can be configured. The key identification numbers need not be consecutive.

Default There are no keys configured on the key chain.

Command Mode key-chain configuration

Usage Guideline Only Routing Information Protocol (RIP) Version 2 uses key chains.

Using the **key** command will enter into the key-chain key configuration mode.

It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid over a period of time. This is based on the **accept-lifetime**, **send-lifetime** and **key chain** key command settings.

If the last key expires, authentication will be invalid.

If there was a discrepancy in the set time of the router's keys, the first valid key will be chosen.

To remove all keys, remove the key chain with the **no key chain** command.

Example

The following example configures a key chain named chain1. Key1 named "forkey1string" will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. Key3 named "forkey3string" will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m.

```
Switch(config)# interface vlan1
Switch(config-if)# ip rip authentication key-chain chain1
Switch(config-if)# ip rip authentication mode text
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 172.19.0.0/8
Switch(config-router)# version 2
Switch(config-router)# exit
Switch(config)# key chain chain1
Switch(config-keychain)# key 1
Switch(config-keychain-key)# key-string forkey1string
Switch(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2009 duration 7200
Switch(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2009 duration 3600
Switch(config-keychain-key)# exit
Switch(config-keychain)# key 3
Switch(config-keychain-key)# key-string forkey3string
Switch(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2009 duration 7200
Switch(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2009 duration 3600
Switch(config-keychain-key)# exit
```

To verify the settings, enter the **show ip key-chain** command.

key chain

To manage authentication keys, define a key chain, identify the keys that belong to the key chain, and specify how long each key is valid by using the **key chain** command. To remove the key chain, use the no form of this command.

key chain *NAME-OF-KEY*

no key chain *NAME-OF-KEY*

Syntax Description	
NAME-OF-KEY	The name used for a key chain (a displayable string). The maximum string length of key chain is 32. If the string includes spaces, then it must be enclosed in quotes (""). A key chain must have at least one key and can have up to 32 keys.

Default No key chains are configured.

Command Mode Global configuration

Usage Guideline Routing Information Protocol (RIP) Version 2 uses key chains for authentication.

To enable authentication, a key chain with named keys must first be created.

It is recommended that only one key chain be configured per interface.

Example

The following example configures a key chain named chain1. Key1 named "forkey1string" will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. Key3 named "forkey3string" will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m.

```
Switch(config)# interface vlan1
Switch(config-if)# ip rip authentication key-chain chain1
Switch(config-if)# ip rip authentication mode text
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 172.19.0.0/8
Switch(config-router)# version 2
Switch(config-router)# exit
Switch(config)# key chain chain1
Switch(config-keychain)# key 1
Switch(config-keychain-key)# key-string forkey1string
Switch(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2009 duration 7200
Switch(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2009 duration 3600
Switch(config-keychain-key)# exit
Switch(config-keychain)# key 3
Switch(config-keychain-key)# key-string forkey3string
Switch(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2009 duration 7200
Switch(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2009 duration 3600
Switch(config-keychain-key)# end
```

To verify the settings, use the **show ip key-chain** command.

key-string

Use the **key-string** command ito specify the authentication string for a key. Use the **no key-string** command to remove the authentication string.

key-string *TEXT*

no key-string [*TEXT* **]**

Syntax Description	
TEXT	The required authentication string sent and received in packets using the routing protocol being authenticated. The string can consist of 1 to 16 alphanumeric characters, the first character cannot be a number.

Default No key chains are configured.

Command Mode key-chain key configuration

Usage Guideline Routing Information Protocol (RIP) Version 2 uses key chains for authentication.

Each key can have only one key string.

Example

The following example configures a key chain named chain1. Key1 named forkey1string will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. Key3 named forkey3string will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m.

```
Switch(config)# interface vlan1
Switch(config-if)# ip rip authentication key-chain chain1
Switch(config-if)# ip rip authentication mode text
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 172.19.0.0/8
Switch(config-router)# version 2
Switch(config)# key chain chain1
Switch(config-keychain)# key 1
Switch(config-keychain-key)# key-string forkey1string
Switch(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2009 duration 7200
Switch(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2009 duration 3600
Switch(config-keychain-key)# exit
Switch(config-keychain)# key 3
Switch(config-keychain-key)# key-string forkey3string
Switch(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2009 duration 7200
Switch(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2009 duration 3600
Switch(config-keychain-key)# end
```

Verify the settings by entering the **show ip key-chain** command.

lacp port-priority

Use the **lacp port-priority** command to configure the port priority. Use the no form to configure the port priority to the default.

lacp port-priority *PRIORITY*

no lacp port-priority

Syntax Description	
PRIORITY	Specifies the port priority. The range is 1 to 65535.

Default 32768

Command Mode Interface configuration

Usage Guideline The **lacp port-priority** command is used to specify which ports can join a port channel and which ports are specified to be in backup mode. In a port priority comparison, a numerically lower value has a higher priority. If two or more ports have the same priority, the port number determines the priority.

Example This example shows how to configure the port priority to 20000 on interface eth3.4 to eth3.5.

```
Switch(config)# interface range eth3.4-3.5
Switch(config-if)# lacp port-priority 20000
```

Verify the settings with the **show channel-group** command.

lacp system-priority

Use the **lacp system-priority** command to configure the system priority used for LACP ports. Use the no form to configure the system priority to the default.

lacp system-priority *PRIORITY*

no lacp system-priority

Syntax Description	
PRIORITY	Specifies the system priority. The range is 1 to 65535.

Default 32768.

Command Mode Global configuration

Usage Guideline During Link Aggregation Control Protocol (LACP) negotiation, the system priority and port priority of the local partner are exchanged with the remote partner. If the maximum number of actual members exceeds the limitation, the switch uses port priority to determine whether the port status will be in backup mode or active mode. The LACP system priority determines which switch controls the port priority for the aggreagated link. The port priorities of the other switch are ignored.

In a system priority comparison, a numerically lower value has a higher priority.

If two switches have the same system priority , the LACP system ID (MAC address) determines the priority.

The LACP system priority command applies to all LACP port channels on the switch.

Example This example shows how to configuration the system priority to 30000.

```
Switch(config)# lacp system-priority 30000
```

Verify the settings with the **show channel-group** command

lease

Use this command to configure the lease duration of an IP address that is assigned from a DHCP server to a client. Use the no form of this command to restore the default value.

lease { *DAYS [HOURS* | *MINUTES*] **| infinite }**

no lease

Syntax Description	
DAYS	Specifies the duration of the lease in number of days
HOURS	(Optional) Specifies the number of hours in the lease. The *DAYS* value must be configured prior to *HOURS*.
MINUTES	(Optional) Specifies the number of minutes in the lease. The *DAYS* and *HOURS* values must be configured prior to *MINUTES*.
Infinite	Specifies the lease is unlimited

Default 1 day

Command Mode DHCP pool configuration

Usage Guideline This command specified the duration of a lease. This command can only be executed under DHCP pool configuration mode, identified by the (config-dhcp)# prompt.

Examples The following is a sample of configuring the lease, in address pool "pool1", to 1 day.

```
switch# configure terminal
switch(config)# ip dhcp pool pool1
switch(config-dhcp)# lease 1
```

The following is sample of configuring the lease, in address pool "pool1", to 1 hour.

```
switch# configure terminal
switch(config)# ip dhcp pool pool1
switch(config-dhcp)# lease 0 1
```

lldp dot1-tlv-select

To specify which optional type-length-value settings (TLVs) in the IEEE 802.1 Organizationally Specific TLV set will be transmitted and encapsulated in the LLDPDUs and sent to neighbor devices, use the lldp dot1-tlv-select command in interface configuration mode. To disable transmit the TLVs, use the **no** form of this command.

lldp dot1-tlv-select { port-vlan | protocol-vlan *VLAN-ID [, | -]* **| vlan-name** *[VLAN-ID [, | -]]* **| protocol-identify [** *PROTOCOL-NAME* **] }**

no lldp dot1-tlv-select { port-vlan | protocol-vlan [*VLAN-ID [, | -]* **] | vlan-name [***VLAN-ID [, | -***]] | protocol-identify [***PROTOCOL-NAME* **] }**

Syntax Description	
port-vlan	Specify the Port Vlan ID TLV to send. The Port VLAN ID TLV is an optional fixed length TLV that allows a VLAN bridge port to advertise the port's VLAN identifier (PVID) that will be associated with untagged or priority tagged frames.
protocol-vlan *VLAN-ID [, | -]*	Specify the Port And Protocol VLAN ID (PPVID) TLV to send. The Port and Protocol VLAN ID TLV is an optional TLV that allows a bridge port to advertise a port and protocol VLAN ID. *VLAN-ID [, | -]* Specify the ID of the VLAN in the PPVID TLV. The VLAN ID range is 1 to 4094. Separate nonconsecutive VLAN-ID with a comma; use a hyphen to designate a range of *VLAN-ID*. In **no** form of this command, the *VLAN-ID [, | -]* is optional. If no *VLAN-ID* is specified, all configured PPVID VLANs will be cleared and no PPVID TLV will be sent.
vlan-name *[VLAN-ID [, | -]*	Specify the VLAN Name TLV to send. The VLAN Name TLV is an optional TLV that allows an IEEE 802.1Q-compatible IEEE 802 LAN station to advertise the assigned name of any VLAN with which it is configured. *VLAN-ID [, | -]* (Optional) Specify the ID of the VLAN in the VLAN Name TLV. The VLAN ID range is 1 to 4094. Separate nonconsecutive *VLAN-ID* with a comma; use a hyphen to designate a range of *VLAN-ID*. If no *VLAN-ID* is specified, all applicable VLANs will be sent. In no form of this command, if no *VLAN-ID* is specified, all configured VLANS for VLAN NAME TLV will be cleared and no VLAN Name TLV will be sent.

Syntax Description	
protocol-identify [*PROTOCOL-NAME*]	Specify the Protocol Identify TLV to send. The Protocol Identify TLV is an optional TLV that allows an IEEE 802 LAN station to advertise particular protocols that are accessible through the port. The valid strings for PROTOCOL-NAME are: **eapol**: Extensible Authentication Protocol (EAP) over LAN **lacp**: Link Aggregation Control Protocol **gvrp**: GARP VLAN Registration Protocol **stp**: Spanning Tree Protocol The *PROTOCOL-NAME* is optional. When no specific protocol string is specified, all protocols are selected or de-selected in no form of the command.

Default No IEEE 802.1 Organizationally Specific TLV is selected.

Command Mode Interface configuration

Usage Guideline If the optional TLVs advertisement state is enabled, they will be encapsulated in LLDPDU and sent to other devices.

The Protocol Identify TLV optional data type indicates whether the corresponding Local System's Protocol Identify instance will be transmitted on the port. The Protocol Identify TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. When both of the protocol function and advertising protocol identify are enabled on a port, the Protocol Identify TLV will be advertised.

Only when the configured VLAN-ID matches the configuration of protocol vlan on that interface and the VLAN exists, then the PPVID TLV for that VLAN will be sent.

Only when the interface is a member port of the configured VLAN-ID, the VLAN will be advertised in VLAN Name TLV.

Example This example shows how to enable advertising Port VLAN ID TLV:

```
Switch(config-if)# lldp dot1-tlv-select port-vlan
```

The following example disables advertising Port VLAN ID TLV:

```
Switch(config-if)# no lldp dot1-tlv-select port-vlan
```

This example shows how to enable advertising Port And Protocol VLAN ID TLV, the advertised VLAN includes 1 to 3.

```
Switch(config-if)# lldp dot1-tlv-select protocol-vlan  1-3
```

The following example disabling Port And Protocol Vlan ID TLV advertisement from valn1 to vlan3

```
Switch(config-if))# no lldp dot1-tlv-select protocol-vlan 1-3
```

This example shows how to enable VLAN Name TLV advertisement from vlan1 to vlan3

```
Switch(config-if)# lldp dot1-tlv-select vlan-name 1-3
```

The following example disables VLAN Name advertisement from valn1 to vlan3

```
Switch(config-if)# no lldp dot1-tlv-select vlan-name 1-3
```

This example shows how to enable LACP Protocol Identify TLV advertisement:

```
Switch(config-if)# lldp dot1-tlv-select protocol-identity lacp
```

This example shows how to disable LACP Protocol Identify TLV advertisement:

```
Switch(config-if)# no lldp dot1-tlv-select protocol-identity lacp
```

lldp dot3-tlv-select

To specify which optional type-length-value settings (TLVs) in the IEEE 802.3 Organizationally Specific TLV set will be transmitted and encapsulated in the LLDPDUs and sent to neighbor devices, use the **lldp dot3-tlv-select** command in Interface Configuration mode. To disable transmit the TLVs, use the no form of this command.

lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | power | max-frame-size]

no lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | power | max-frame-size]

Syntax Description

mac-phy-cfg	(Optional) Specify the MAC/PHY Configuration/Status TLV to send. The MAC/PHY Configuration/Status TLV is an optional TLV that identifies: ■ The duplex and bit-rate capability of the sending IEEE 802.3 LAN node. ■ The current duplex and bit-rate settings of the sending IEEE 802.3 LAN node.
link-aggregation	(Optional) Specify the Link Aggregation TLV to send. The Link Aggregation TLV indicates contains the following information: ■ Whether the link is capable of being aggregated. ■ Whether the link is currently in an aggregation. ■ The aggregated port channel ID of the port. If the port is not aggregated, then the ID is 0.
power	(Optional) Specify the Power via MDI TLV to send. Three IEEE 802.3 PMD implementations (10BASE-T, 100BASE-TX, and 1000BASE-T) allow power to be supplied over the link for connected non-powered systems. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station.
max-frame-size	(Optional) Specify the Maximum Frame Size TLV to send. The Maximum Frame Size TLV indicates the maximum frame size capability of the implemented MAC and PHY.
	When no optional keyword is selected, all supported IEEE 802.3 Organizationally Specific TLVs are selected or de-selected in no form of this command.

Default No IEEE 802.3 Organizationally Specific TLV is selected.

Command Mode Interface configuration.

Usage Guideline The **lldp dot3-tlv-select** command enables the advertisement of the optional IEEE 802.3 Organizationally Specific TLVs. The respective TLV will be encapsulated in LLDPDU and sent to other devices if the advertisement state is enabled.

Example This example shows how to enable advertising MAC/PHY Configuration/Status TLV:

```
Switch (config-if) # lldp dot3-tlv-select mac-phy-cfg
```

This example shows how to disable advertising MAC/PHY Configuration/Status TLV:

```
Switch (config-if) # no lldp dot3-tlv-select mac-phy-cfg
```

lldp fast-count

To set the LLDP-MED fast start repeat count on the switch, use the **lldp fast-count** command. Use the no form of this command to return to the default settings.

lldp fast-count VALUE

no lldp fast-count

Syntax Description	
VALUE	The valid range is from 1 to 10.

Default 4 times

Command Mode Global configuration mode.

Usage Guideline When an LLDP-MED Capabilities TLV is detected, the application layer shall start fast start mechanism. This command is used to configure the fast start repeat count which indicates the number of LLDP message transmissions for one complete fast start interval.

Example This example shows how to set LLDP MED fast start repeat count:

```
Switch(config)# lldp fast-count 10
```

lldp hold-multiplier

To set the hold multiplier for LLDP updates on the switch, use the lldp hold-multiplier command. Use the no form of this command to return to the default settings.

lldp hold-multiplier *VALUE*

no hold-multiplier

Syntax

VALUE	Specifies a multiplier on the LLDPDUs transmission interval that used to compute the time to live value of an LLDPDU; valid values are from 2 to 10.

Default 4

Command Mode Global configuration

Usage Guideline This parameter is a multiplier on the LLDPDUs transmission interval that used to compute the TTL value in an LLDPDU. The lifetime is determined by hold-multiplier times tx-interval and up to 65535. At the partner switch, when the time-to-live for a given advertisement expires, the advertised data is deleted from the neighbor switch's MIB.

Example This example shows how to set LLDP hold-multiplier to 3:

```
Switch(config)# lldp hold-multiplier 3
```

This example shows how to set LLDP hold-multiplier to default value.

```
Switch(config)# no lldp hold-multiplier
```

lldp management-address

To configure management address which will be advertised on the physical interface, use the lldp management-address command. Use the no form of this command to remove the settings.

lldp management-address [*IP-ADDRESS* **|** *IPV6-ADDRESS* **]**

no lldp management-address [*IP-ADDRESS* **|** *IPV6-ADDRESS* **]**

Syntax Description	
IP-ADDRESS	(Optional) The IPv4 address which is carried in Management Address TLV.
IPV6-ADDRESS	(Optional) The IPv6 address which is carried in Management Address TLV.
	When no IPv4 or IPv6 address is input for the command **lldp management-address**, the swicth will find the least IP/IPv6 address if the smallest VLAN.

Default No LLDP management address is configured (no Management Address TLV is sent)

Command Mode Interface configuration

Usage Guideline

The command is available for physical port configuration. This command specifies the IPv4/IPv6 address which is carried in Management Address TLV on the specified port. If an IP address is specified, but the address is not one of the addresses of system interfaces, then the address will not be sent.

When no optional address specified along the command **lldp management address**, the switch will find least IP and IPv6 address of the VLAN with the smallest VLAN ID, as default IP and IPv6 address respectively. If no applicable IP/IPv6 address, no management address TLV will be advertised. Once user configures an address (no matters what it is IP or IPv6 address), both of the default IP and IPv6 management address become inactive and won't be sen t. The default IP or IPv6 address will be active again when the configured address is removed. Multiple IP/IPv6 management addresses can be configured by setting this command multiple times.
Use the command no lldp management-address without specifying management address to disable management address advertising in LLDPDUs.
If there is no management address in the list, no Management Address TLV will be sent.

Example This example shows how to enable eth3.1 and eth3.2 for setting management address entry (ipv4)

```
Switch(config-if)# interface range eth3.1-3.2
Switch(config-if)# lldp management-address 10.1.1.1
```

This example shows how to enable eth3.3 and eth3.4 for set management address entry (ipv6)

```
Switch(config)# interface range eth3.3-3.4
Switch(config-if-range)# lldp management-address FE80::250:A2FF:FEBF:A056
```

This example shows how to delete the management address 10.1.1.1 on eth3.1 and eth3.2. If 10.1.1.1 is the last one, no Management Address TLV will be sent.

```
Switch(config)# interface range eth3.1-3.2
Switch(config-if-range)# no lldp management-address 10.1.1.1
```

This example shows how to delete the management address FE80::250:A2FF:FEBF:A056 on eth3.3 and eth3.4.

```
Switch(config)# interface range eth3.3-3.4
Switch(config-if-range)# no lldp management-address
FE80::250:A2FF:FEBF:A056
```

This example shows how to delete all management address(es) on eth3.5 and then no Management Address TLV will be sent on eth3.5.

```
Switch(config)# interface eth3.5
Switch(config-if-range)# no lldp management-address
```

lldp med-tlv-select

To specify which optional **LLDP-MED TLV** will be transmitted and encapsulated in the LLDPDUs and sent to neighbor devices, use the lldp med-tlv-select command in Interface configuration mode. To disable transmit the TLVs, use the **no** form of this command.

lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management]

no lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management]

Syntax Description	
capabilities	(Optional) Transmits 'LLDP-MED Capabilities TLV'. If user wants the physical interface transmit LLDP-MED TLVs, this TLV type should be enabled. Otherwise, the interface cannot transmit any LLDP-MED TLVs.
inventory-management	(Optional) Transmits 'LLDP-MED Inventory Management TLV'.
network-policy	(Optional) Transmits 'LLDP-MED Network Policy TLV'.
power-management	(Optional) Transmits 'LLDP-MED Extended Power-via-MDI TLV' if local device is PSE device or PD device. When no optional keyword is selected, all supported optional LLDP-MED TLVs are selected or de-selected in **no** form of this command.

Default No LLDP-MED TLV is selected.

Command Mode Interface configuration mode

Usage Guideline This command is used to enable or disable transmitting LLDP-MED TLVs.

Only when voice vlan is enabled, the port is the member of voice vlan and network-policy is selected, then LLDP-MED Network Policy TLV can be advertised from the interface.

If you disable transmitting Capabilities TLV, LLDP-MED on the physical interface

will be disabled at the same time. In other words, all LLDP-MED TLVs will not be

sent, even other LLDP-MED TLVs are enabled to transmit.

By default, the switch only sends LLDP packets until it receives LLDP-MED packets from the end device. The switch continues to send LLDP-MED packets until it only receives LLDP packets.

Example This example shows how to enable all TLVs:

```
Switch(config-if)# lldp med-tlv-select
```

This example shows how to enable transmitting LLDP-MED TLVs and LLDP-MED Capabilities TLV will be sent:

```
Switch(config-if)# lldp med-tlv-select capabilities
```

This example shows how to enable transmitting LLDP MED Inventory Management TLV:

```
Switch(config-if)# lldp med-tlv-select inventory-management
```

lldp receive

To enable a physical interface to receive LLDP message, use the lldp receive command in Interface Configuration mode. Use the no form of this command to disable receiving LLDP message.

lldp receive

no lldp receive

Syntax This command has no arguments or keywords.

Default LLDP is enabled on all supported interfaces.

Command Mode Interface Configuration mode

Usage Guideline This command is used to enable a physical interface to receive LLDP message. When LLDP is not running (when the command **no lldp run** is issued on global configuration mode), the switch doesn't receive LLDP message.

Example This example shows how to enable a physical interface to receive LLDP message.

```
Switch(config-if)# lldp receive
```

This example shows how to disable a physical interface to receive LLDP message.

```
Switch(config-if)# no lldp receive
```

lldp reinit

To set the minimum time of re-initialization delay interval on the switch, use the **lldp reinit** command. Use the **no** form of this command to return to the default settings.

lldp reinit SECONDS

no lldp reinit

Syntax Description

SECONDS	Specifies a delay for LLDP initialization on an interface; valid values are from 1 to 10 seconds.

Default 2 seconds

Command Mode Global configuration

Usage Guideline A re-enabled LLDP physical interface will wait for re-initialization delay after last disable command before reinitializing.

Example This example shows how to set the re-init delay interval to 5 seconds.

```
Switch(config)# lldp reinit 5
```

This example shows how to set the re-init delay interval to default value.

```
Switch(config)# no lldp reinit
```

lldp run

To enable Link Layer Discovery Protocol (LLDP) globally, use the **lldp run** command in global configuration mode. Use the no form of this command to return to the default settings.

lldp run

no lldp run

Syntax This command has no arguments or keywords.

Default LLDP global state is disabled.

Command Mode Global configuration

Usage Guideline This is a global control for the LLDP function.

You can use **lldp run** in global configuration mode to globally enable LLDP, and then the switch can start to transmit LLDP packets and receive and process the LLDP packets. However, the transmission and receiving of LLDP can be controlled respectively by the command lldp transmit and lldp receive in interface configuration mode. LLDP takes effect on a physical interface only when it is enabled both globally and on the physical interface.

By advertising LLDP packets, the switch announces the information to its neighbor through physical interfaces. On the other hand, the switch will learn the connectivity and management information from the LLDP packets advertised from the neighbor(s).

Example This example shows how to globally enable LLDP:

```
Switch(config)# lldp run
```

This example shows how to globally disable LLDP.

```
Switch(config)# no lldp run
```

lldp tlv-select

To select optional type-length-value (TLVs) in the 802.1AB basic management set will be transmitted and encapsulated in the LLDPDUs and sent to neighbor devices, use the **lldp tlv-select** command in Interface Configuration mode. To disable transmit the TLVs, use the **no** form of this command.

lldp tlv-select [port-description | system-capabilities | system-description | system-name]

no lldp tlv-select [port-description | system-capabilities | system-description | system-name]

Syntax Description

port-description	(Optional) Specify the Port Description TLV to send. The Port Description TLV allows network management to advertise the IEEE 802 LAN station's port description.
system-capabilities	(Optional) Specify the System Capabilities TLV to send. The System Capabilities field shall contain a bit-map of the capabilities that define the primary function(s) of the system.
system-description	(Optional) Specify the System Description TLV to send. The System Description should include the full name and version identification of the system's hardware type, software operating system, and networking software.
system-name	(Optional) Specify the System Name TLV to send. The System Name should be the system's fully qualified domain name.
	When no optional keyword is selected, all supported optional 802.1AB basic management TLVs are selected or de-selected in **no** form of this command.

Default No optional 802.1AB basic management TLV is selected.

Command Mode Interface Configuration

Usage Guideline The command is available for physical port configuration.
The **lldp tlv-select** command is used to select the optional TLVs to be transmitted. If the optional TLVs advertisement is selected, they will be encapsulated in LLDPDU and sent to other devices.

Examples This example shows how to enable all supported optional 802.1AB basic management TLVs:

```
Switch(config-if)# lldp tlv-select
```

This example shows how to enable advertising System Name TLV:

```
Switch(config-if)# lldp tlv-select system-name
```

This example shows how to disable advertising System Name TLV:

```
Switch(config-if)# no lldp tlv-select system-name
```

lldp transmit

To enable the LLDP advertise (transmit) capability, use the **lldp transmit** command in Interface Configuration mode. Use the no form of this command to disable LLDP transmission.

lldp transmit

no lldp transmit

Syntax This command has no arguments or keywords.

Default LLDP transmit is enabled on all supported interfaces.

Command Mode Interface Configuration mode

Usage Guideline This command is used to enable LLDP transmission on a physical interface. When LLDP is not running (when the command **no lldp run** is issued on global configuration mode), the router doesn't transmit LLDP message.

Example This example shows how to enable LLDP transmission.

```
Switch(config-if)# lldp transmit
```

This example shows how to disable LLDP transmission.

```
Switch(config-if)# no lldp transmit
```

lldp tx-delay

To set the transmission delay timer use the **lldp tx-delay** command. This delay timer defines the minimum interval between sending of LLDP messages due to constantly change of MIB content. Use the no form of this command to return to the default settings.

lldp tx-delay SECONDS

no lldp tx-delay

Syntax Description

SECONDS	Specifies a delay for sending successive LLDPDU on an interface; valid values are from 1 to 8192 seconds and should not greater than one-fourth of transmission interval timer

Default 2 seconds

Command Mode Global configuration

Usage Guideline The LLDP transmission interval (tx-interval) must be greater than or equal to four times of transmission delay timer.

Example This example shows how to set the transmission delay timer to 8 seconds.

```
Switch(config)# lldp tx-delay 8
```

The following example configures the transmission delay timer to default value.

```
Switch(config)# no lldp tx-delay
```

lldp tx-interval

To set the LLDPDUs transmission interval on the switch, use the **lldp tx-interval** command. Use the **no** form of this command to return to the default settings.

lldp tx-interval SECONDS

no lldp tx-interval

Syntax Description

SECONDS	Specifies the interval between consecutive transmissions of LLDP advertisements on each physical interface. The range is from 5 to 32768 seconds.

Default 30 seconds

Command Mode Global configuration

Usage Guideline This interval controls the rate at which LLDP packets are sent.

Examples This example shows how to set LLDP updates are sent every 50 seconds.

```
Switch(config)# lldp tx-interval 50
```

This example shows how to set LLDP transmission interval to default value:

```
Switch(config)# no lldp tx-interval
```

logging file

Use the **logging file** command to enable the storage of log messages to FLASH memory from the logging buffer.

logging file

Syntax None

Default None

Command Mode Global configuration

Usage Guideline Use this command to save log messages from the logging buffer to flash.

Example The example below sets log messages to be saved to flash.

```
Switch> enable
Switch# configure terminal
Switch(config)# logging  file
```

logging host

Use the **logging host** command to log system messages to a remote host. Remove logging hosts from the configuration with the **no logging host** command.

logging host *IPADDRESS* **[port** *UDP-PORT***] [severity {emergency |alert |critical |error |warning |notice |informational|debugging}] [facility {local0|local1| local2| local3| local4| local5| local6| local7}]**

no logging host [*IP-ADDRESS* **]**

Syntax Description		
IP-ADDRESS	Specifies the IP address of the host to be used as the syslog server. IPv4 and IPv6 address are supported.	
port *UDP-PORT*	(Optional) The UDP port number to be used for the syslog server. Valid values are 514 or any value from 1024 to 65535.	
severity	(optional) Specifies the severity of log messages that will be sent to the server.	
	emergency	System is unusable.
	alert	Action must be taken immediately.
	critical	critical condition
	error	error conditions
	warning	warning condition
	notice	normal but significant condition
	informational	informational message
	debugging	debugging message
facility	(optional) Specifies the facility (refer to options listed in the below rows) in the log messages to be sent to the server.	
	local0	local use 0
	local1	local use 1
	local2	local use 2
	local3	local use 3
	local4	local use 4
	local5	local use 5
	local6	local use 6
	local7	local use 7

Default

IP-ADDRESS: None

UDP port: 514.

severity: informational

facility: local7

Command Mode Global configuration

Usage Guideline The number of supporting SYSLOG servers is project dependent. When the number of configured SYSLOG servers reaches the maximum capacity, a new SYSLOG server is unable to be configured before and existing entry is deleted using the command **no logging host**.

The severity level limits the logging of system messages sent to Syslog servers to only those messages at and up to the specified level. For example, if the severity is debugging, all logs in the Syslog daemon are sent to the log server host. If the level of log is alert, then only alert and emergency logs are sent.

The keyword facility specifies the syslog facility in the SYSLOG messages which are sent to the server.

For the no command, if the IP address is not specified, all logging hosts will be deleted.

Example The below example shows how to create a log server with the host address 20.3.3.3 . The command configures the server to receive logs with a severity level set to critical

```
Switch> enable
Switch# configure terminal
Switch(config)# logging host  20.3.3.3 severity critical
```

Verify the settings with the **show logging host** command.

logging level

Use this command to limit messages logged to the message buffer based on severity level.

logging level all *SEVERITY*

Syntax Description	
all	All facilities
SEVERITY	Value for the severity level of system messages to capture. Severity level definitions are shown in the following table.

Severity Level	Severity Type	Description
0	emergency	system is unusable
1	alert	action must be taken immediately
2	critical	critical conditions
3	error	error conditions
4	warning	warning conditions
5	notice	normal but significant condition
6	informational	informational messages
7	debugging	debugging messages

Default *SEVERITY*: 5

Command Mode Global configuration

Usage Guideline The command limits the logging of system messages to the syslog buffer to only those messages for the specified facility at and up to the specified severity level. For example, if the buffer severity is 7 (debugging) then all logs in syslog daemon will log to buffer. If buffer severity is 1 (alert), then only alert and emergency logs will be logged to buffer.

Example The below example limits logs with severity alert and emergency to be logged to buffer for all facilities.

```
switch> enable
switch# configure terminal
Switch(config)# logging level all 1
```

Verify the settings by entering the **show logging** command.

logging on

Use the **logging on** command to start logging system messages on this switch. Use the no form of this command to stop logging.

logging on

no logging on

Syntax None

Default Logging of system messages is on.

Command Mode Global configuration

Usage Guideline To enable logging of system messages, use the **logging on** command in global configuration mode.

Example To set logging of system messages to on, execute the below commands.

```
Switch> enable
switch# configure terminal
Switch(config)# logging on
```

Verify the settings with the **show logging** command.

login

Use this command to login to the switch with a specified username.

login

Syntax None

Default None

Command Mode User EXEC

Usage Guideline Change a login username by using this command.

When logging in using a TELNET connection, if all of the attempts fail, the connection will be returned to the logout state. For a direct console connection, the session will also be returned to the logout state.

Example This example shows how to login with username user1.

```
Switch>login

User Access Verification

Username: user1
Password:

                    DGS-6604 Chassis-based High-Speed Switch
                             Command Line Interface

                                Firmware: 1.00.029
          Copyright (c) 2011 D-Link Corporation. All rights reserved.
Switch#
```

logout

Use this command to close an active terminal session by logging off the switch.

logout

Syntax None

Default None

Command Mode User EXEC

Usage Guideline Close an active terminal session by logging off the device using the **logout** command.

Example This example shows how to logout from the switch.

```
Switch# disable
Switch> logout
```

loopback-detection (interface)

Use the command to enable interface loopback detection function. Use the **no** form to disable the function.

loopback-detection

no loopback-detection

Syntax None

Default Disabled

Command Mode Interface mode

Usage Guideline The command is available for port and port channel interface configuration.

When a port enables the loopback-detection function, and switch is in forwarding state, will periodically sends out CTP packets with the SA field set to device's MAC, DA field set to CF-00-00-00-00-00. Type is "90-00". If the port is an untagged member of a VLAN, this port will send out the untagged CTP packet. If the port is only tagged member of VLAN, then this port will send out the tagged packet with one of the VLAN ID to which this port belonged.

When the switch detects that a CTP packet sent out by the port has been looped back to the packet originating port, it will put this port into error disabled state or block the traffic which belong to this VLAN according to the detection mode user configured.

There are two kinds of recovery mechanisms provide, user can bring it out of this state by entering the "errdisable recovery cause loopback-detection" global configuration command. Alternatively, the user can manually re-enable the port by entering the "shutdown" then "no shutdown" command in interface-configuration mode.

The LBD will work only when both the global setting and port setting are enabled.

Prompt Message

Prompt message at screen	Description
Cannot enable LBD on the port as it is STP enabled.	STP and LBD should be mutual exclusive on the same port.

Example This example shows how to enable loopback detection function on port3.1

```
Switch(config)# interface eth3.1
Switch(config-if)# loopback-detection
Switch(config-if)#
```

You can verify your settings by entering the show loopback-detection command.

loopback-detection (global)

Use the command to enable global loopback detection function. Use **no** form to disable the function.

loopback-detection

no loopback-detection

Syntax None

Default Disabled

Command Mode Configuration mode

Usage Guideline Used to enable or disable the LBD function globally.

When a port enables the loopback-detection function, and switch is in forwarding state, will periodically sends out CTP packets with the SA field set to device's MAC, DA field set to CF-00-00-00-00-00. Type is "90-00". If the port is an untagged member of a VLAN, this port will send out the untagged CTP packet. If the port is only tagged member of VLAN, then this port will send out the tagged packet with one of the VLAN ID to which this port belonged.

When the switch detects that a CTP packet sent out by the port has been looped back to the packet originating port, it will put this port into error disabled state or block the traffic which belong to this VLAN according to the detection mode user configured. There are two kinds of recovery mechanisms provide, user can bring it out of this state by entering the "errdisable recovery cause loopback-detection" global configuration command. Alternatively, the user can manually re-enable the port by entering the "shutdown" then "no shutdown" command in interface-configuration mode.

Example This example shows how to enable loopback detection function.

```
Switch(config)# loopback-detection
Switch(config)#
```

You can verify your settings by entering the show loopback-detection command.

loopback-detection mode

Use the command to decide the loopback detection mode. To return to the default settings, use the no form of this command.

loopback-detection mode {port-based | vlan-based}

no loopback-detection mode

Syntax

port-based	In the port-based mode, the port will enter the error disabled state when detects the loop
vlan-based	In VLAN-based mode, the port can't process packets of the VLAN that detects the loop.

Default The default mode is port-based.

Command Mode Configuration mode

Usage Guideline If the detection mode is set to port-based means the switch determines loopback based on port. If loop back happened, will treat the whole port as loop backed port and block this port. LBD will send the CTP packets periodically per port.

On the other side, vlan-based mode makes switch will per port per VLAN send the CTP packets periodically. This mode can detect loopback based on VLAN. If switch detects loopback on a VLAN, LBD will only block the traffic which belongs to this VLAN. Other VLANs' traffic should not be affected on this port.

Example This example shows how to choose the loopback detection operation mode:

```
Switch(config)# loopback-detection mode vlan-based
Switch(config)#
```

You can verify your settings by entering the show loopback-detection command.

loopback-detection interval-time

Use the command to configure timer interval. Use no command to return the default settings.

loopback-detection interval-time SECONDS

no loopback-detection interval-time

Syntax

Interval-time *SECONDS*	The time interval (in seconds) at which device transmits all the CTP (Configuration Test Protocol) packets to detect the loop-back event. Valid range is from 1 to 32767.

Default The default setting is 10 seconds.

Command Mode Configuration mode

Usage Guideline The timer interval of the device will transmit the CTP (Configuration Test Protocol) packets periodically to detect a loop-back event. If the loopback detection mode is port-based, LBD will per port send the CTP packets. Oppositely, LBD will per port per VLAN send the CTP packets periodically on VLAN base mode.

Example This example shows how to configure the time interval.

```
Switch# configure terminal
Switch(config)# loopback-detection interval-time 20
Switch(config)#
```

You can verify your settings by entering the show loopback-detection command.

mac access-group

Use the **mac access-group** command to specify a MAC access list to be applied to an interface. Use the **no mac access-group** command to remove the access group control from the interface.

mac access-group *NAME* **[in]**

no mac access-group *NAME* **[in]**

Syntax Description	
NAME	The name of the MAC access list to be applied. Up to 32 characters are allowed. The syntax is a general string that does not allow spaces.
in	Specifies that the MAC access list will be applied in the ingress direction.

Default If the **in** direction is not specified, the default will be the **in** direction.

Command Mode Interface configuration

Usage Guideline Only one MAC access list can be applied to the same interface. An error message is sent if an attempt is made to apply a second MAC access list and the attempt is ignored.

The MAC access list must first be created using the **mac access-list** command before it can be applied to interface. Otherwise, an error message will be displayed.

The keyword **in** specifies the ingress direction check.

One MAC access-list, one IP access-list and one IPv6 access-list can be applied to the same interface.

The association of an access-group with an interface will consume the filtering entry resource in the switch controller. If the command is applied successfully, the number of remaining max entries will be displayed. If the resource is insufficient to commit the command, an error message will be displayed.

Example This example shows applied MAC access-list “daily-profile” to eth3.1

```
Switch(config)# interface eth3.1
Switch(config-if)# mac access-group daily-profile in
```

Verify the settings with the **show access-group** command.

mac access-list

Use the **mac access-list** command to create a MAC access list in the configuration. Enter this command to go into **mac access-list** configuration mode. Use the no form of the command to delete a MAC access list.

mac access-list extended *NAME*

no mac acces-list extended *NAME*

Syntax Description	
NAME	The name of the MAC access list being created. The syntax is a general string with no spaces of up to 32 characters.

Default An implicit deny statement for all addresses.

Command Mode Global configuration

Usage Guideline To apply an access list to an interface, create the list with the **mac access-list extended** command. An interface can have only one MAC access list, one IP access list and one IPv6 access list applied to it. Use this command to enter the **mac access-list** configuration mode, then use the **permit/deny** command to specify the entries.

Access lists names must be unique among access lists. Access list names are case sensitive.

A configured access list is always terminated by an implicit deny statement for all addresses.

An error message will appears if the allowed number of lists is exceeded.

If both a MAC access list and an IP access-list or IPv6 access-list are applied to an interface, the packet will be processed using the MAC access list first. If the packet is not dropped by the MAC access list, the packet will be then processed by the IP access list or the IPv6 access list. This order of packet handling therefore gives higher priority to the MAC access list.

Example This example shows how to enter the mac access-list configuration mode for “daily-profile”:

```
Switch(config)# mac access-list extended daily-profile
Switch(config-mac-ext-acl)#
```

Verify the access list configuration settings with the **show access-list** command.

mac address-table aging destination-hit

Use the MAC address-table aging destination-hit command to enable the destination MAC address triggered update function (Updates the hit bit of the MAC address entry based on the destination MAC of the forwarding packet).

Use the no form of the command to disable the triggered updated function.

mac address-table aging destination-hit

no mac address-table aging destination-hit

Syntax None

Default Disabled

Command Mode Global configuration

Usage Guideline The source MAC address triggered update function is always enabled. When a user enables the destination MAC address triggered update function by entering the "mac address-table aging destination-hit" command, the hit bit of MAC address entries will be updated. It will be updated for either the destination MAC addresses or the source MAC addresses when the forwarding packet is matched. The destination MAC address triggered update function increases the frequency of the MAC address entries hit bit update and will reduce the traffic flooding when the aging of MAC address entries expires.

Example This example shows how to enable the destination MAC address triggered update function.

```
Switch:15(config)# mac address-table aging destination-hit
```

Verify the setting by entering the **show mac address-table aging destination-hit** command.

mac address-table aging-time

Use this command to set the length of time that a dynamic entry remains in the MAC address table.

mac address-table aging-time *SECONDS*

Syntax Description	
SECONDS	Aging time in seconds. The valid range is 0 or 10 to 1000000 seconds. 0 means that the aging function is disabled so entries never age out.

Default *SECONDS*: 300

Command Mode Global configuration

Usage Guideline Set the aging time to 0 to disable the MAC address table aging out function.

Example This example shows how to set the aging time to 200 seconds:

```
Switch(config)# mac address-table aging-time 200
```

Verify the setting by entering the **show mac address-table aging-time** command.

mac address-table static

Use the **mac address-table static** command to add a static address to the MAC address table. Use the **no mac address-table static** command to remove static addresses from the table.

mac address-table static *MAC-ADDR* **vlan** *VLAN-ID* **interface** *INTERFACE-ID* **[, | -]**

no mac address-table static *MAC-ADDR* **vlan** *VLAN-ID* **[interface** *INTERFACE-ID* **] [, | -]**

Syntax Description	
MAC-ADDR	Destination MAC address (unicast or multicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface. The acceptable formats are 00-01-80-40-30-20, 00:01:80:40:30:20, 000180403020, and 0001.8040.3020.
vlan *VLAN-ID*	Specifies the VLAN which will receive the packet with the specified MAC address destination. The range is 1 to 4094.
interface *INTERFACE-ID*	Specifies the interface to which received packets are forwarded to. Both physical ports and port-channels are valid.

Default Not configured

Command Mode Global configuration

Usage Guideline A unicast MAC address entry can be specified with only one interface.

A multicast MAC address entry can be specified with multiple interfaces.

To delete a unicast MAC address entry, it is not necessary to specify the interface ID. When deleting a multicast MAC address entry, if the interface ID is specified, only that interface is removed. Otherwise, the entire multicast MAC entry will be removed.

An error message will appear if the entry to be removed does not exist.

Example This example shows how to add static address C2:F3:22:0A:12:F4 to the MAC address table. When a packet is received in VLAN 4, with this MAC address as its destination, the packet is forwarded to the specified interface:

```
Switch(config)# mac address-table static C2:F3:22:0A:12:F4 vlan 4 interface
eth3.1
```

Verify the setting by entering the **show mac address-table** command.

mac-base (VLAN)

Use the **mac-base** command to create a MAC-based VLAN ID assignment entry. Use the no form of this command to remove a MAC-based VLAN ID assignment entry.

mac-base *MAC-ADDRESS*

no mac-base *MAC-ADDRESS*

Syntax Description	
MAC-ADDRESS	Specifies the MAC address for the entry.
VLAN-ID	Specifies the VLAN ID for the entry.

Default Not configured

Command Mode VLAN configuration

Usage Guideline Use the mac-base command to create a MAC-based VLAN ID assignment entry. Any frame with a source MAC address matching the entry is classified as a member of the VLAN associated with the entry.

Example This example shows how to create a MAC-based VLAN ID entry.

```
Switch(config)#vlan 101
Switch(config-vlan)#mac-base 00-80-cc-00-00-11
Switch(config-vlan)#exit
```

Verify the settings with the **show vlan** command.

match

Use the match command in the class map configuration mode to configure the match criteria for a class-map. Use the no form of the command to remove the match criteria.

match {access-list *ACCESS-LIST-NAME* **| cos** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **| [ip] precedence** *IP-PRECEDENCE-LIST*] **| protocol** *PROTOCOL-NAME* **| vlan VLAN-LIST}**

no match { access-list *ACCESS-LIST-NAME* **| cos** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **| [ip] precedence** *IP-PRECEDENCE-LIST*] **| protocol** *PROTOCOL-NAME* **| vlan** *VLAN-ID-LIST***}**

Syntax Description	
access-list *ACCESS-LIST-NAME*	Name of an access-list that will be used as the match criteria. The only allowed access-list is the ip access-list with a permit rule to class the pass-through traffic, other traffic is not classified for any QoS service.
cos *COS-LIST*	Specific IEEE 802.1Q CoS value. The COS_LIST is from 0 to 7; Enter one or more CoS values separated by commas.
dscp *DSCP-LIST*	Numbers (0 to 63) representing differentiated services code point values. Enter one or more differentiated service code point (DSCP) values separated by commas.
precedence *IP-PRECEDENCE-LIST*	Numbers (0 to 7) representing the IP precedence values. Enter one or more precedence values separated by commas.
protocol *PROTOCOL-NAME*	Name of the protocol (for example, bgp) used as a matching criterion. See the "Usage Guidelines" for a list of protocols supported by most routers.
vlan *VLAN-ID-LIST*	VLAN identification number, numbers, or range of numbers. Valid VLAN identification numbers must be in the range of 1 to 4094.

Default Not configured

Command Mode Class-map configuration

Usage Guideline To use the match command, the user must first enter the class-map command to specify the name of the class to establish the match criteria with. The treatment of these matched packets is defined by the user through the setting of Quality of Service (QoS) policies in the policy-map class configuration mode.

The match access-list command specifies a named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the class. The packets that are permitted by the access list will be included in the class.

To match a packet on the basis of a Layer 2 class of service (CoS) marking, use the **match cos** command in class-map configuration mode. To remove a specific Layer 2 CoS marking as a match criterion, use the no form of this command.

To identify one or more differentiated service code point (DSCP), use the **match dscp** command in class-map configuration mode. To remove a specific DSCP

value from a class map, use the no form of this command. As an example for the **match dscp** command, if the user wants to match the DCSP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values needs to be matched, not all of the specified DSCP values), enter the match dscp 0,1,2,3,4,5,6,7 command. This command is used by the class map to identify the specified DSCP value on a packet as a match with the traffic class configured.

To identify IP precedence values to use as the match criteria, use the **match precedence** command in class-map configuration mode. To remove IP precedence values from a class map, use the no form of this command. For example, to use the precedence values of 0, 1, 2, or 3 (note that only one of the precedence values needs to be matched, not all of the specified precedence values), enter the match ip precedence 0,1.2.3 command or match ip precedence 0-3 command.

To configure the match criteria for a class map on the basis of the specified protocol, use the **match protocol** command in class-map configuration mode. To remove protocol-based match criterion from a class map, use the no form of this command.

To match and classify traffic on the basis of the virtual local-area network (VLAN) identification number, use the **match vlan** command in class-map configuration mode. To remove a previously specified VLAN identification number as a match criterion, use the no form of this command

The match protocol command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class.

Supported Protocols:

The following table lists the reference for the supported protocols.

Protocol	Description
arp	IP Address Resolution Protocol (ARP)
bgp	Border Gateway Protocol
dhcp	Dynamic Host Configuration
dns	Domain Name Server lookup
egp	Exterior Gateway Protocol
ftp	File Transfer Protocol
ip	IP (version 4)
netbios	NetBIOS
nfs	Network File System
ntp	Network Time Protocol
ospf	Open Shortest Path First
pppoe	Point-to-Point Protocol over Ethernet
rip	Routing Information Protocol
rtsp	Real-Time Streaming Protocol

Protocol	Description
ssh	Secured shell
telnet	Telnet
tftp	Trivial File Transfer Protocol

Examples The following example specifies a class map called class-home-user and configures the access list named acl-home-user to be used as the match criteria for that class:

```
Switch(config)# class-map class-home-user
Switch(config-cmap)# match access-list acl-home-user
Switch(config-cmap)# exit
```

In the following example, classes called voice and video-n-data are created to classify traffic based on the CoS values. QoS treatment is then given to the appropriate packets in the cos-based-treatment policy map (in this example, the QoS treatment is a single rate policer and a two rate policer for class voice and video-n-data respectively). The service policy configured in this example is attached to Ethernet interface eth3.1.

```
Switch(config)# class-map voice
Switch(config-cmap)# match cos 7
Switch(config-cmap)# exit
Switch(config)# class-map video-n-data
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
Switch(config)# policy-map cos-based-treatment
Switch(config-pmap)# class voice
Switch(config-pmap-c)# police 8000 1000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video-n-data
Switch(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000
exceed-action drop violate-action drop
exceed-action  2 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface eth3.1
Switch(config-if)# service-policy cos-based-treatment
```

The following example specifies a class map called cos and specifies that the CoS values of 1, 2, and 3 are match criteria for the class:

```
Switch(config)# class-map cos
Switch(config-cmap)# match cos 1,2,3
Switch(config-cmap)# exit
```

Verify the settings by entering the **show class-map** command.

match as-path

Use this command to match a BGP autonomous system path access list. To delete an entry, use the **no** form of this command.

match as-path *ACCESS-LIST-NAME*

no match as-path *ACCESS-LIST-NAME*

Syntax Description	
ACCESS-LIST-NAME	Specifies the name of AS path access list.

Default Not configured

Command Mode Route-map configuration

Usage Guideline The values set by the **match as-path** and set weight commands override global values. For example, the weights assigned with the **match as-path** and **set weight route-map** configuration commands override the weight assigned using the neighbor weight command.

A route map can have several parts. Any route that does not match at least one match clause relating to a route-map command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. To modify only a portion of the data, a second route-map section must be configured with an explicit match statement.

match means that the AS path list exactly matches the AS path, or is a subset of the AS path list.

Example This example shows how to add a match statement to the policy routing entry with name myPolicy:

```
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match as-path PATH_ACL
```

Verify the settings with the **show route-map** command.

match community

Use the **match community** command to match a Border Gateway Protocol (BGP) community. Use the **no match community** command to remove the entry from the list and return to the default condition.

match community *COMMUNITY-LIST-NAME* **[exact]**

no match community *COMMUNITY-LIST-NAME* **[exact]**

Syntax Description	
COMMUNITY-LIST-NAME	The name of the community list.
exact	(Optional) Requires an exact match. All of the communities specified must be present and no other communities are allowed.

Default Not configured

Command Mode Route-map configuration

Usage Guideline A route is not advertised for outbound route maps or accepted for inbound route maps if the route does not match at least one match clause relating to a route-map command. In order to modify only a portion of the route data it is necessary to configure a second route-map section that specifies an explicit match.

Matching based on the community list number is one of the types of match commands applicable to BGP.

This route map set command is only for BGP.

When exact is specified, the communities of the route must be exactly the same as the permited communities specified in the community-list (by the command ip community-list).

When exact is not specified, at least one community of the route must match one of the permited communities in the community-list, and that community does not match any deny community.

Example In the following example, routes that match the community list ALPHA-COMMUNITY, which is 101:200, have their weights then set to 100. Any route that has community 101:200 alone (exact match) will have its weight set to 100.The route policy is named myPolicy:

```
Switch(config)#ip community-list ALPHA-COMMUNITY permit 101:200
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match community ALPHA-COMMUNITY exact
Switch(config-route-map)# set weight 100
```

Verify the settings with the **show route-map** command

match ip address

Use this command to define a clause to match the route based on IP standard access list.

match ip address *ACCESS-LIST-NAME*

no match ip address [*ACCESS-LIST-NAME*]

Syntax Description	
ACCESS-LIST-NAME	Specify a standard or an extended IP access list name.

Default Not configured

Command Mode Route-map configuration

Usage Guideline Use the **match ip address** command in route map configure mode to define rule for matching routes against IP standard access list.

Example The following example create an IP access list "myacl" first and create a route map entry to match against the create IP access list.

```
Switch(config)# ip access-list myacl
Switch(config-ip-acl) # permit 10.20.0.0 255.255.0.0 any
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match ip address myacl
```

You can verify your settings by entering the **show route map** command.

match ipv6 address

Use this command to define a clause to match the route based on IPv6 access list.

match ipv6 address *IPv6-ACCESS-LIST-NAME*

no match ipv6 address **[***IPv6-ACCESS-LIST-NAME***]**

Syntax Description	
IPv6-ACCESS-LIST-NAME	Specify an IPv6 access list name.

Default Not configured

Command Mode Route-map configuration

Usage Guideline Use the **match ipv6 address** command in route map configure mode to define rule for matching routes against IP standard access list.

Example The following example create an IP access list "aclv6cfg" first and create a route map entry to match against the create IP access list.

```
Switch(config)# ipv6  access-list extended aclv6cfg
Switch(config-ip-acl) # permit 2000::3:4 ffff::0 any
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match ipv6 address aclv6cfg
```

You can verify your settings by entering the **show route map** command.

maximum-paths

To control the maximum number of parallel routes that an IP routing protocol can support, use the maximum-paths command in router configuration mode.

maximum-paths *NUMBER-PATHS*

Syntax Description	
NUMBER-PATHS	Maximum number of parallel routes that an IP routing protocol installs in a routing table; valid values are from 1 to 8.

Default *NUMBER-PATHS*: 6

Command Mode Global configuration

Usage Guideline None

Example The following example shows how to allow a maximum of 8 paths to a destination for an Open Shortest Path First (OSPF) routing process::

```
Router(config)# maximum-paths 8
```

Verify the settings by entering the **show ip route summary** command.

max-rcv-frame-size

Use the command to set the maximum Ethernet frame size allowed. Use the default form to restore the default max-rcv-frame-size size.

max-rcv-frame-size BYTES

default max-rcv-frame-size

Syntax Description	
BYTES	Set the maximum Ethernet frame size allowed. The range is 1536 to 9728 bytes.

Default *BYTES:* 1536 bytes

Command Mode Interface command for physical port and port channel but not for VLAN.

Usage Guideline Oversize frames will be dropped and the check is done within the ingress ports.

Use the command to transfer large frames or jumbo frames through the switch system to optimize server-to-server performance.

When a port is removed from the port-channel member list, the max-rcv-frame-size setting for the port will be reset to the default setting.

Examples This example shows how to set max-rcv-frame-size as 6000 bytes at eth4.1

```
Switch# configure terminal
Switch(config)# interface eth4.1
Switch(config-if) max-rcv-frame-size 6000
Switch(config-if)# end
```

This example shows how to restore the default max-rcv-frame-size

```
Switch# configure terminal
Swtich(config)# interface eth4.1
Switch(config-if)# default max-rcv-frame-size
Switch(config-if)# end
```

Verify the settings by entering the **show interface** command.

mgmt-if

Use this command to enter into the management interface mode. Commands entered in this mode will be applied to the management port.

mgmt-if

Syntax None

Default None

Command Mode Global configuration

Usage Guideline None

Example The following example displays how to enter the management interface mode.

```
Switch(config)# mgmt-if
Switch(mgmt-if)#
```

Verify the settings using the **show mgmt-if** command.

monitor session

Use **monitor session** to create a port mirroring session, allowing source ports as mirrored ports to be monitored through a destination port. Use the no form of this command to delete all or a specific port mirroring session, or remove either a destination port or a source port within a specific port mirroring session.

monitor session *SESSION-NUMBER* **destination interface** *INTERFACE-ID* **[***ingress***]**

no monitor session *SESSION-NUMBER* **destination interface** *INTERFACE-ID*

no monitor session [*SESSION-NUMBER* **]**

Syntax Description	
SESSION-NUMBER	Specifies the session number identified with the port mirroring session. The valid range is 1 to 80.
destination	Specifies the port mirroring destination. A destination can be a physical port or a port channel.
source	Specifies the port mirroring source. A source can be a physical port or a port channel.
interface *INTERFACE-ID*	Specifies the destination or source interface for a port mirroring session. For both source and destination interfaces, physical ports and port-channel interfaces are valid interface types.
[*ingress***]**	(Optional) Specify to enable processing of packets received on the destination port. By default, the received packet is not processed.

Default Not configued

Command Mode Global configuration

Usage Guideline The following applies to monitoring:

- A desination port and source port cannot be the same port.
- A port-channel can be specified as a monitor source or as a monitor destination.
- A channel-group member port cannot be specified as a monitor source port or destination port.
- For a monitor session, multiple source interfaces can be specified. However, only one destination interface can be specified. An interface cannot be a source interface of one session and destination port of another session simultaneously.
- For a destination port, all the layer 2 settings configured for this port are all ineffective.

- IEEE 802.1x authentication on a port cannot be enabled for a destination port, but is allowed on the source port.

Entering **no monitor session** without specifying a session number deletes all port mirroring sessions.

Examples

This example shows how to create a port mirroring session with session number 1. It assigns a physical port (eth3.1) as a destination port and three source physical ports (eth3.2, eth3.3, and eth3.4) as mirrored ports.

```
Switch# configure terminal
Switch(config)# monitor session 1 destination interface eth3.1
Switch(config)# monitor session 1 source interface eth3.2-3.4
Switch(config)# end
```

This example shows how to remove two source ports from a created port mirroring session with session number 1.

```
Switch# configure terminal
Switch(config)# no monitor session 1 source interface eth3.2,eth3.4
Switch(config)# end
```

Verify the settings by entering the **show monitor session** command.

monitor session destination remote vlan

Use the command to configure the RSPAN VLAN and destination port for a RSPAN source session. Use the no form of the command to remove configuration of the RSPAN VLAN.

monitor session *SESSION-NUMBER* **destination remote vlan** *VLAN-ID* **interface** *INTERFACE-ID*

no monitor session *SESSION-NUMBER* **destination remote vlan**

Syntax Description	
SESSION-NUMBER	Specify the session number for the port monitor session. The valid range is 1 to 80.
remote vlan *VLAN-ID*	Specify the RSPAN VLAN used to tunnel the monitored packets to the remote site. The valid range is 2 to 4094.
interface *INTERFACE-ID*	Specify the interface to transmit the monitored packets to the remote site.

Default Not configured

Command Mode Global configuration mode

Usage Guideline Use the command on the source switch of a RSPAN session.

The monitor session destination remote vlan command configures the destination port used to transmit the monitor packets and the RSPAN VLAN used to tunnel the monitored packets to the remote site. The destination port does not need to be the member port of the RSPAN VLAN. The destination port can be either a physical port or a port channel.

Use the monitor session source interface command to configure the source ports whose packets will be monitored.

Use the remote-span command in vlan config mode to specify a VLAN as a RSPAN VLAN. When a VLAN is specified as a RSPAN VLAN, the access member port of the VLAN will become inactive. The monitor packet will be tunneled over the trunk member port of the RSPAN VLAN.

The RSPAN VLAN is a tunnel VLAN. The source port does not need to be member ports of the RSPAN VLAN.

Example This example shows how to create a RSPAN session on the source switch. It assigns VLAN 100 as the RSPAN VLAN with destination interface eth3.6 and three source ports (eth 2.2, eth 2.3 and eth 2.4) as the port being monitored:

```
Switch# configure terminal
Switch(config)# vlan 100
Switch(config-vlan)# remote-span
Switch(config-vlan)#exit
Switch(config)# monitor session 2 source interface eth2.2-2.4
Switch(config)# monitor session 2 destination remote vlan 100 interface
eth3.6
Switch(config)#
```

You can verify your settings by entering the **show monitor session** command.

monitor session source interface

Use monitor session source interface to configure the source port of a port monitor session. Use the no form of this command to remove all or a port monitor session, or remove a source port from the port monitor session.

monitor session SESSION-NUMBER source interface *INTERFACE-ID* **[, | -] [both | rx | tx]**

no monitor session SESSION-NUMBER source interface *INTERFACE-ID* **[, | -] [both | rx | tx]**

no monitor session [SESSION-NUMBER]

Syntax Description	
SESSION-NUMBER	Specify the session number for the port monitor session. The valid range is 1 to 80.
source interface *INTERFACE-ID*	Specify the source interface for a port monitor session.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.
both, **rx**, **tx**	(Optional) Specifies the traffic direction to monitor. If not specified, the source interface sends both transmitted and received traffic.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.

Default No port monitor function is configured.

Command Mode Global configuration

Usage Guideline Both physical ports and port channel are valid as source interfaces of monitor sessions. The physical port that is a port channel member port cannot be specified as the source interface.

For a monitor session, multiple source interfaces can be specified, but only one destination interface can be specified. An interface can not be a source interface of one session and destination port of another session simultaneously. An interface can be configured as destination interface of multiple sessions, but it can be a source interface of only one session.

If direction is not specified, both transmitted and received traffic are monitored.

If no monitor session is entered without specifying a session number, all port monitor sessions are deleted.

Example This example shows how to create a port monitor session with session number 1. It assigns a physical port 2.1 as a destination port and three source physical ports (eth 2.2, eth 2.3 and eth 2.4) as monitor source ports.

```
Switch# configure terminal
Switch(config)# monitor session 1 destination interface eth2.1
Switch(config)# monitor session 1 source interface eth2.2-2.4
Switch(config)#
```

This example shows how to remove two source ports from port monitor session 1.

```
Switch# configure terminal
Switch(config)# no monitor session 1 source interface eth2.2,eth2.4
Switch(config)#
```

You can verify your settings by entering the **show monitor session** command.

monitor session source remote vlan

Use the command to configure the RSPAN VLAN for a RSPAN destination session. Use the no form of the command to remove configuration of the RSPAN VLAN.

monitor session *SESSION-NUMBER* **source remote vlan** *VLAN-ID*

no monitor session *SESSION-NUMBER* **source remote vlan**

Syntax Description	
SESSION-NUMBER	Specify the session number of the port mirroring session. The valid range is 1 to 80.
remote vlan *VLAN-ID*	Specify the VLAN that the monitored source packets are tunneled over from the remote site. The valid range is 2 to 4094.

Default Not configured

Command Mode Global configuration mode

Usage Guideline Use the command on the destination switch of a RSPAN session.

The monitor session source remote vlan command configures the VLAN that the monitored source packets are tunneled over from the remote site. Use the monitor session destination interface command to configure the destination port.

Use the remote-span command in vlan config mode to specify a VLAN as a RSPAN VLAN. When a VLAN is specified as a RSPAN VLAN, the access member port of the VLAN except the destination interface will become inactive.

Example This example shows how to create a RSPAN session on the destination switch. It assigns VLAN 100 as the RSPAN VLAN and eth1.4 as the destination port. It also assigns VLAN 100 as the RSPAN VLAN. The monitored packets arrive at port eth2.1 and will be transmitted out from port eth1.4.

```
Switch# configure terminal
Switch(config)# vlan 100
Switch(config-vlan)# remote-span
Switch(config-vlan)#exit
Switch(config)# interface eth2.1
Switch(config-vlan)# trunk-allowed vlan 100
Switch(config-vlan)# exit
Switch(config)# interface eth2.4
Switch(config-vlan)# access vlan 100
Switch(config-vlan)# exit
Switch(config)# monitor session 2 source remote vlan 100
Switch(config)# monitor session 2 destination interface eth2.4
Switch(config)#
```

mtu

Use the command to set the MTU value. This value is used to monitor oversize IP packets. Use default form to restore to the default mtu size.

mtu *BYTES*

default mtu

Syntax Description	
BYTES	Set the monitor threshold. The settable range is 1280 to 9692 bytes.

Default *BYTES:* 1500 bytes

Command Mode Interface command for physical port and port channel but not for VLAN.

Usage Guideline Oversize packets will be sent to the control module blade for further processing and the check is done in egress ports. This is especially important to support IPv6 because an IPv6 router should send out ICMP messages to source device for an MTU violation situation.

As a port is removed from the port-channel member list, the MTU setting for the port will be reset to the default setting.

One should set appropriate values to these MTUs to avoid unexpected results. In the general case, max- rcv-frame-size is larger than the ip mtu and mtu to cover L2 header size. **mtu** is set as the same value as ip mtu.

Examples This example shows how to set mtu as 6000 bytes at eth4.1

```
Switch# configure terminal
Switch(config)# interface eth4.1
Switch(config-if) mtu 6000
Switch(config-if)# end
```

This example shows how to restore the default mtu

```
Switch# configure terminal
Swtich(config)# interface eth4.1
Switch(config-if)# default mtu
Switch(config-if)# end
```

Verify the settings by entering the **show interface** command

multicast filtering-mode

Use the **multicast filtering mode** command to configure the method how an interface handles unknown multicast packets.

multicast filtering-mode { forward-all | forward-unregistered | filter-unregistered }

Syntax Description	
forward-all	Flood all multicast packets based on VLAN domain.
forward-unregistered	Forward the registered multicast packet based on forwarding table, and flood all un-registered multicast packets based on VLAN domain.
filter-unregistered	Forward the registered packets based on forwarding table, and filter all un-registered multicast packets.

Default **forward-unregistered**

Command Mode Interface configuration

Usage Guideline Only VLAN interfaces support this command.

Example This example shows how to set the multicast filtering mode to filter-unregistered.

```
Switch(config)# interface vlan1
Switch(config-if)# multicast filtering-mode filter-unregistered
```

Verify the setting by entering the **show multicast filtering-mode** command.

name

Use the **name** command to set the name of an MST region. To return to the default name, use the no form of this command.

name *NAME*

no name

Syntax Description	
NAME	The name given for a specified MST region. The name string has a maximum length of 32 characters and the type is a general string which allows spaces.

Default *NAME*: (The MAC Address of the Bridge)

Command Mode MST configuration

Usage Guideline If two or more switches have the same VLAN mapping and configuration version number, the switches are considered to be in different MST regions if the region names are different. Use the **name** command to differenciate MST regions.

Caution: Use care when the name command is used to set the name of an MST region. A mistake can put the switch in a wrong or different region. The MST region name is a case-sensitive parameter.

Example This example shows how to configure the MSTP configuration name to 'alpha'.

```
Switch(config)#spanning-tree mst configuration
Switch(config-mst)# name alpha
```

Verify the settings by entering the **show spanning-tree mst configuration** command.

neighbor

Use the **neighbor** command to define a neighboring router with which to exchange routing information. Use the no form to remove an entry.

neighbor *IP-ADDRESS*

no neighbor *IP-ADDRESS*

Syntax Description	
IP-ADDRESS	IP address of a peer router with which routing information will be exchanged.

Default Not configured

Command Mode Router configuration

Usage Guideline This command allows point-to-point (non-broadcast) exchange of routing information. Additional neighbors or peers can be specified using multiple **neighbor** commands.

When used in combination with the **passive-interface** router configuration command, routing information can be exchanged between a subset of routers and access servers on a LAN.

Example In the following example, RIP updates are sent to all interfaces except vlan1 on network 10.0.0.0/8. However, in this case a neighbor router configuration command is included. This command permits routing updates to be sent to specific neighbors. One copy of the routing update is generated per neighbor:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0/8
Switch(config-router)# passive-interface vlan1
Switch(config-router)# neighbor 10.50.71.50
```

Verify the settings by entering the **show ip protocols rip** command

neighbor (RIP IPv6)

To define a neighboring router with which to exchange routing information, use the **neighbor** command in router configuration mode. Use the no form of the command to remove an entry.

neighbor *IPv6-ADDRESS IFNAME*

no neighbor *IPv6-ADDRESS IFNAME*

Syntax Description	
IPv6-ADDRESS	IPv6 link-local address of a router with which routing information will be exchanged.
IFNAME	The specified interface type and interface number

Default Not configured

Command Mode Router configuration

Usage Guideline This command permits the point-to-point exchange of routing information.

Multiple neighbor commands can be used to specify additional neighbors or peers.

When it is used in combination with the passive-interface router configuration command, routing information can be exchanged between a subset of routers and access servers on a LAN.

Example In the following example, RIPng updates are sent to a specified interface vlan1 on fe80::1. This command permits routing updates to be sent to specific neighbors. One copy of the routing update is generated per neighbor:

```
Switch# configure terminal
Switch(config)# router ipv6 rip
Switch(config-router)# neighbor fe80::1 vlan1
```

Verify the settings by entering the **show ipv6 rip database** command

neighbor advertisement-interval

Use this command to set the minimum interval between each transmission of Border Gateway Protocol (BGP) routing updates. Use the no form of the command to return to the default configuration.

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

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

Syntax Description	
IP-ADDRESS	Specifies IP address prefixes.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group.
SECONDS	The interval, in seconds, between each transmission of UPDATE messages. The range is from 1 to 600.

Default *SECONDS*: 30 seconds for external peers

SECONDS: 5 seconds for internal peers

Command Mode Address family configuration

Router configuration

Usage Guideline When a BGP peer group is specified using the PEER-GROUP-NAME argument, all the members of the peer group inherit the characteristic configured with this command.

Example The following address family configuration mode example sets the minimum time between sending BGP routing updates to 15 seconds:

```
Switch(config)# router bgp 65100
Switch(config-router)# address-family ipv4
Switch(config-router-af)# neighbor 10.4.4.4 advertisement-interval 15
```

Verify the settings by entering the **show ip bgp neighbor** command.

neighbor description

Use this command to associate a text description with a neighbor. Use the no form of the command to remove the description.

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

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

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

Default None

Command Mode Router configuration

Usage Guideline When a BGP peer group is specified using the PEER-GROUP-NAME argument, all the members of the peer group inherit the characteristics configured with this command.

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 description ABC in China
```

Verify the settings by entering the **show ip bgp neighbor** command.

neighbor filter-list

Use this command to create a BGP filter. Use the no form of the command to disable this function.

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

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

Syntax Description	
IP-ADDRESS	Specifies the IP address prefix.
PEER-GROUP-NAME	The name of a Border Gateway Protocol (BGP) peer group.
AS-PATH-LIST-NAME	The name of an autonomous system path access list. Define this access list with the **ip as-path access-list** command.

Default Disabled

Command Mode Router configuration

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

Each neighbor can only have 1 **in** and 1 **out** access list.

Example The following example shows how to configure the BGP neighbor with IP address 172.16.1.1 to not send advertisements about any path which is through or from the adjacent autonomous system 123:

```
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)# router bgp 65100
Switch(config-router)# network 10.108.0.0
Switch(config-router)# neighbor 192.168.6.6 remote-as 123
Switch(config-router)# neighbor 172.16.1.1 remote-as 47
Switch(config-router)# neighbor 172.16.1.1 filter-list myacl out
```

Verify the settings, in User Exec Mode, by entering the **show ip protocols bgp** command.

neighbor peer-group (create group)

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

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

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

Syntax Description	
PEER-GROUP-NAME	Name of the BGP peer group

Default Not configured

Command Mode Router configuration

Address family configuration

Usage Guideline Often in a BGP or multiprotocol BGP speaker, multiple neighbors are configured with the same update policies (that is, the same outbound route maps, distribution lists, filter lists, update source, and so on).

Neighbors with the same update policies can be grouped into peer groups to simplify configuration and make update calculations more efficient.

Example This example shows how to create a peer group named ALPHA-GROUP

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

neighbor peer-group (add group member)

Use this command to add a neighbor into a peer group. Use the no form of the command to remove a neighbor from a peer group.

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

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

Syntax Description	
IP-ADDRESS	IP address of the neighbor.
PEER-GROUP-NAME	Name of the BGP peer group

Default None

Command Mode Router configuration

Address family configuration

Usage Guideline The neighbor at the specified IP address inherits all the configured options of the peer group.

Example This example shows how to add a group member 10.1.1.254 to the peer group, named ALPHA-GROUP.

```
Switch(config)# router bgp 65100
Switch(config-router)# neighbor ALPHA-GROUP peer-group
Switch(config-router)# neighbor 10.1.1.254 peer-group ALPHA-GROUP
```

Verify the settings by entering the **show ip bgp neighbor** command in User EXEC mode.

neighbor remote-as

Use this command to add an entry to the Border Gateway Protocol (BGP) neighbor table. Use the **no** form of this command to remove an entry from the table.

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

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

Syntax Description	
IP-ADDRESS	IP address of the neighbor.
PEER-GROUP-NAME	The Name of a BGP peer group.
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 65536 to 4294967295 or 1.0 to 65535*65535.

Default Not configured

Command Mode Router configuration

Usage Guideline Use this command to add the IP address of the neighbor, in the specified autonomous system, to the BGP neighbor table of the local router.

Specifying a neighbor with an autonomous system number, that matches the autonomous system number specified in the router bgp global configuration command, identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor will be considered as external.

When a BGP peer group is specified using the PEER-GROUP-NAME argument, all the members of the peer group inherit the characteristics configured with this command.

By default, neighbors that are defined using the neighbor remote-as command in router configuration mode exchange only unicast address prefixes.

Example This example shows how to specify a router with the address 10.108.2.1 as a neighbor in autonomous system number 110:

```
Switch(config)# router bgp 65100
Switch(config-router)# network 10.108.0.0
Switch(config-router)# neighbor 10.108.2.1 remote-as 110
```

Verify the settings by entering the **show ip bgp neighbor** command.

neighbor route-map

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

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

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

Syntax Description	
IP-ADDRESS	Specifies IP address prefixes.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group.
MAP-NAME	Name of the route map.
out	Applies the route-map to the outgoing routes.

Default None

Command Mode Address family configuration

Router configuration

Usage Guideline When issued in address family configuration mode, this command applies a route map to that particular address family only. When issued in router configuration mode, this command applies a route map to IP Version 4 unicast routes only.

If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map.

When a BGP peer group is specified using the *PEER-GROUP-NAME* argument, all the members of the peer group inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

Example The following example in router configuration mode applies a route map named internal-map to a BGP outgoing route from 172.16.70.24:

```
Switch(config)#router bgp 5
Switch(config)#neighbor 172.16.70.24 route-map internal-map out
Switch(config)#route-map internal-map permit 10
Switch(config-route-map)#match as-path 1
Switch(config-route-map)#set origin incomplete
Swtich(config-route-map)#end
Switch(config)#
```

Verify the settings by entering the **show ip bgp neighbor** command.

neighbor send-community

Use this command to specify that the communities attribute should be sent to a BGP neighbor, 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 prefixes.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group.
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 Address family configuration

Router configuration

Usage Guideline When a BGP peer group is specified using the *PEER-GROUP-NAME* argument, then all the members of the peer group inherit the characteristics configured with this command.

Example The following example, using the address family configuration mode, sets the send-community with the **both** option (standard and extended):

```
Switch(config)# router bgp 65100
Switch(config-router)# address-family ipv4
Switch(config-router-af)# neighbor 10.4.4.4 send-community both
```

Verify the settings by entering the **show ip bgp neighbor** command.

neighbor shutdown

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

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

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

Syntax Description	
IP-ADDRESS	Specifies IP address prefixes.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group.

Default None

Command Mode Router configuration

Usage Guideline Use this command to terminate any active session for the specified neighbor or peer group and remove all associated routing information. In the case of a peer group, a large number of peering sessions could be suddenly terminated.

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
```

Verify the settings by entering the **show ip bgp neighbor** command.

neighbor timers

Use this command to set the timers for a specific BGP peer or peer group. Use the no form of this command to clear the timers for a specific BGP neighbor.

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 prefixes.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group.
KEEP-ALIVE	The frequency (in seconds) that specifies how often the switch sends keepalive messages to its peer. The default is 60 seconds. The range is from 0 to 65535.
HOLD-TIME	The elapsed time (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

Usage Guideline The timers configured for a specific neighbor, or peer group, override the timers configured for all BGP neighbors using the **timers bgp** command.

Example The following example shows how to configure the *KEEP-ALIVE* timer to 120 seconds and the *HOLD-TIME* timer to 360 seconds for the neighbor 172.16.10.10:

```
Switch(config)# router bgp 65100
Switch(config-router)# neighbor 172.16.10.10 timer 120 360
```

Verify the settings by entering the **show ip bgp neighbor** command.

neighbor update-source

Use this command to allow internal 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-ID*

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} update-source** *INTERFACE-ID*

Syntax Description	
IP-ADDRESS	Specifies IP address prefixes
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group
INTERFACE-ID	Specifies the interface ID

Default The best local address is used.

Command Mode Router configuration

Usage Guideline Use this command in conjunction with any specified interface on the router.

Example The following example shows how to configure the internal BGP sessions to use VLAN 1 for the neighbor 172.16.10.10:

```
Switch(config)# router bgp 65100
Switch(config-router)# neighbor 172.16.10.10 update-source vlan1
```

Verify the settings by entering the **show ip bgp neighbor** command.

neighbor weight

Use this command to specify the weight 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 prefixes.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group.
weight *NUMBER*	Weight to assign. Acceptable values are from 0 to 65535.

Default Routes learned through another BGP peer have a default weight: 0

Routes sourced by the local router have a default weight: 32768.

Command Mode Address family configuration

Router configuration

Usage Guideline The weight specified by this command determines the weight to be associated with the routes learned from a specified neighbor.

Example The following address family configuration mode example sets the weight of the neighbor 10.4.4.4 to 10000:

```
Switch(config)# router bgp 65100
Switch(config-router)# address-family ipv4
Switch(config-router-af)# neighbor 10.4.4.4 weight 10000
```

Verify the settings by entering the **show ip bgp neighbor** command.

netbios node-type

This command is used to configure the NetBIOS node's type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients. Use the no form of this command to restore the configuration of the NetBIOS node's type back to default configuration (Hybrid).

netbios node-type *NTYPE*

no netbios node-type

Syntax Description	
NTYPE	Specifies the type of NetBIOS node. Valid types are listed below: • b-node - Broadcast • p-node - Peer-to-peer • m-node - Mixed • h-node - Hybrid (recommended)

Default *NTYPE*: h-node

Command Mode DHCP pool configuration

Usage Guideline This command configures the NetBIOS node's type; the recommended type is h-node (Hybrid). It determines what methods NetBios will use to register and resolve names.

- **b-node** - The broadcast system uses broadcasts.
- **p-node** - A p-node system uses only point-to-point name queries to a name server (WINS).
- **m-node** - An m-node system broadcasts first, and then queries the name server.
- **Hybrid** - A hybrid system queries the name server first, and then broadcasts.

Resolution through LMHOSTS and/or Domain Name Service (DNS), if enabled, will follow these methods.

Example The following is sample of configuring the Netbios node type as h-node.

```
switch# configure terminal
switch(config)# ip dhcp pool pool1
switch(config-dhcp)# netbios node-type h-node
```

netbios scope-id

This command configures the NetBIOS scope id for Microsoft Dynamic Host Configuration Protocol (DHCP) clients. Use the no form of this command to remove the configuration of NetBIOS scope id.

netbios scope-id *STRING*

no netbios scope-id

Syntax Description	
STRING	A character string. The maximum length is 18 characters.

Default None

Command Mode DHCP pool configuration

Usage Guideline The Scope ID is a character string which is appended to the NetBIOS name for all NetBIOS communications over TCP/IP. It provides a method to isolate a collection of computers that can then only communicate with each other.

Example The following is sample of configuring the NetBIOS Scope ID as the string “alpha”.

```
switch#configure terminal
switch(config)#ip dhcp pool pool1
switch(config-dhcp)#netbios scope-id alpha
switch(config-dhcp)#
```

netbios wins-server

To configure the IP address of a WINS server for Microsoft Dynamic Host Configuration Protocol (DHCP) clients. Use the no form of this command to remove the configuration of WINS server.

netbios wins-server *IP-ADDRESS*

no netbios wins-server [*IP-ADDRESS***]**

Syntax Description	
IP-ADDRESS	The IP address of the WINS server.

Default Not configured

Command Mode DHCP pool configuration

Usage Guideline This command is used to configure a primary and secondary WINS server. The primary preference is the old WINS. The maximum number of configurable WINS servers is dependent on each project.

Examples The following example configures a primary WINS server as 10.1.1.100.

```
switch(config-dhcp)#netbios wins-server 10.1.1.100
```

The following example configures a secondary WINS server as 10.1.1.200.

```
switch(config-dhcp)#netbios wins-server 10.1.1.200
```

The following example removes the WINS server 10.1.1.100 so that 10.1.1.200 becomes the primary WINS server.

```
switch(config-dhcp)#no netbios wins-server 10.1.1.100
```

network

Use the command to specify that the network utilizes Routing Information Protocol (RIP). To remove an RIP network entry, use the no form of this command.

network *NETWORK-PREFIX I MASK*

no network *NETWORK-PREFIX I MASK*

Syntax Description	
NETWORK-PREFIX / MASK	The network prefix and the prefix length specify the destination network in the form of xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx or xxx.xxx.xxx.xxx/x. Example: 10.9.18.2 255.0.0.0 or 10.9.18.2/8

Default Not configured

Command Mode Router configuration

Usage Guideline Use this command to specify networks to which routing updates are sent and received. If a network is not specified, the interfaces in that network will not be advertised in any RIP update.

Example The following example shows how to define RIP as the routing protocol to be used on all interfaces connected to networks 192.168.70.0/24 and network 10.99.0.0/16

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# network 192.168.70.0/24
Swtich(config-router)# network 10.99.0.0/16
Switch(config-router)# end
```

Verify the settings by entering the **show ip protocols rip** command.

network (BGP)

Use this command to configure the networks to be advertised by the Border Gateway Protocol (BGP) protocol. To remove an entry from the routing table, use the **no** form of this command.

network { *NETWORK-NUMBER* [*/SUBNET-LENGTH*] | *NETWORK-NUMBER* [mask *NETWORK-NUMBER*] } [route-map *MAP-TAG*]

no network { *NETWORK-NUMBER* [*/SUBNET-LENGTH*] | *NETWORK-NUMBER* [mask *NETWORK-NUMBER*] } [route-map *MAP-TAG*]

Syntax Description	
NETWORK-NUMBER	Specifies the number of the network that BGP will advertise.
*SUBNET-LENGTH**	(Optional) Specifies the prefixlength of the network or sub-network.
mask *NETWORK-NUMBER**	(Optional) Specifies the network or sub-network mask with a mask address.
route-map *MAP-TAG*	(Optional) Specifies the identifier 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.

*** Note:** Specification of the sub-network can be in the form of a subnet mask or a stated length. It is recommened to use the subnet mask form as xxx.xxx.xxx.xxx which is similar to Windows or Linux OS setting. However, that form will be interchangable between for example, 10.9.18.2/8 and 10.9.18.2 255.0.0.0.

Default None

Command Mode Router configuration

Address family configuration

Usage Guideline BGP networks are 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; this will then add 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.

When the synchronized state is enabled, BGP advertises a network entry if the router has the route information for the entry

Example The following example sets up network 10.108.0.0 to be included in the BGP updates for the AS number of 65100

```
Switch(config)# router bgp 65100
Switch(config-router)# network 10.108.0.0
```

network area

Use this command to enable OSPF routing with a specified Area ID. It enables this routing on interfaces with IP addresses that match the specified network address. Use the no parameter with this command to remove the configuration and disable OSPF routing on the interfaces.

network *SUBNET-PREFIX/ SUBNET-MASK-LENGTH* **area** *AREA-ID*

network *SUBNET-PREFIX SUBNET-MASK* **area** *AREA-ID*

no network *SUBNET-PREFIX/ SUBNET-MASK-LENGTH* **area** *AREA-ID*

no network *SUBNET-PREFIX SUBNET-MASK* **area** *AREA-ID*

Syntax Description	
SUBNET-PREFIX	Specifies the address A.B.C.D IPv4 network prefix.
SUBNET-MASK-LENGTH	Specifies the IPv4 network prefix length.
SUBNET-MASK	Specifies the subnet mask used by the network.
AREA-ID	Specifies the identifier of the area for which a VLAN interface is to be enabled. The identifier can be specified as either an IP address or a decimal value.

Default None

Command Mode Router configuration

Usage Guideline OSPF routing can be enabled per IPv4 subnet basis. Each subnet can belong to one particular OSPF area. Network addresses can be defined using the prefix length or a wild card mask.

If there are conflicts, error messages will be returned.

Example The following example shows how to define OSPF area 3 for the interfaces belonging to 10.0.0.0/8:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# network 10.0.0.0/8 area 3
```

Verify the settings with the **show ip ospf** command.

next-server

Configure the next server in a DHCP client's boot process. Use the no form of this command to remove the boot server list.

next-server *IP-ADDRESS*

no next-server

Syntax Description	
IP-ADDRESS	The IP address of next-server in a DHCP client's boot process.

Default Not configured

Command Mode DHCP pool configuration

Usage Guideline The configured IP addresses of next-server are used as a boot server in the DHCP client's boot process. Typically, servers are Trivial File Transfer Protocol (TFTP) servers and are listed in order of preference.

Example The following is a sample of configuring 10.1.1.1 as the IP address of next-server in the DHCP client's boot process in pool named "pool1"

```
switch# configure terminal
switch(config)# ip dhcp pool pool1
switch(config-dhcp)# next-server 10.1.1.1
```

passive-interface

Use the **passive-interface** command to disable sending OSPF protocol packets on an interface. To re-enable sending and receiving routing updates, use the no form of this command.

passive-interface *IFNAME*

no passive-interface *IFNAME*

Syntax Description	
IFNAME	Specifies a layer 3 interface (VLAN).

Default Routing updates are sent on the interface.

Command Mode Router configuration

Usage Guideline The valid interface for this configuration is VLAN.

If an interface is passive, no adjacency can be formed on the passive interface and the OSPF protocol packets are not sent or received through the specified interface. However, the network of the passive interface will be advertised through another non-passive interface.

Example This command shows how to set interface VLAN 1 to the passive mode.

```
Switch# configure terminal
Switch (config)# router ospf
Switch(config-router)##passive-interface vlan1
```

Verify the settings by entering the **show ip ospf interface** command.

passive-interface (IPv6 OSPF)

To disable sending IPv6 OSPF protocol packets on an interface, use the **passive-interface** command. To re-enable sending and receiving routing updates, use the no form of this command.

passive-interface *IFNAME*

no passive-interface *IFNAME*

Syntax Description	
IFNAME	Interface type and number i.e VLAN 1.

Default

Routing updates are sent and received on all interfaces where the routing protocol is enabled.

No interfaces are configured as passive.

Command Mode

Router configuration

Usage Guideline

If the sending of routing updates is disabled on an interface, the particular address prefix will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

IPv6 OSPF routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the IPv6 OSPF domain.

Example

The following example sets interface VLAN 1 to the passive mode:

```
Switch > enable
Switch # configure terminal
Switch (config) # router ipv6 ospf
Switch (config-router)# passive-interface vlan1
```

Verify the settings by entering the **show ipv6 ospf interface** command.

passive interface (RIP)

To disable sending routing updates on an interface, use the **passive-interface** command. To re-enable sending routing updates, use the no form of this command.

passive-interface *IFNAME*

no passive-interface *IFNAME*

Syntax Description	
IFNAME	Specifies the Interface type and Interface number.

Default Routing updates are sent on the interface.

Command Mode Router configuration

Usage Guideline If the sending of routing updates is disabled on an interface, the particular subnet will continue to be advertised to other interfaces. In addition, updates from other routers on that interface will continue to be received and processed.

Examples The following example shows how to disable sending routing updates on the interface VLAN 1:

```
Switch# configure terminal
Switch(config)#router rip
Switch(config-router)# passive-interface vlan1
Switch(config-router)#exit
Switch(config)#
```

Verify the settings by entering the **show ip rip interface** command.

passive-interface (RIP IPv6)

To disable sending routing updates on an interface, use the passive-interface command . To re-enable sending routing updates, use the no form of this command.

passive-interface *IFNAME*

no passive-interface *IFNAME*

Syntax Description	
IFNAME	Specifies the Interface type and Interface number.

Default Routing updates are sent on the interface.

Command Mode Router configuration

Usage Guideline If the sending of routing updates is disabled on an interface, the particular subnet will continue to be advertised to other interfaces. In addition, updates from other routers on that interface will continue to be received and processed.

Example The following example shows how to disable sending routing updates on the interface VLAN 1:

```
Switch# configure terminal
Switch(config)#router ipv6 rip
Switch(config-router)# passive-interface vlan1
Switch(config-router)#exit
```

Verify the settings by entering the **show ipv6 rip interface** command.

password recovery

To configure the security password recovery mechanism, use the password recovery command.

password-recovery

Syntax None

Default None

Command Mode reset configuration.

Usage Guideline It is necessary to authenticate a user for access management. The pairing of username and password is a basic authenticating mechanism. **'Password Recovery'** provides administrators a handle for the scenario of administrators wanting to update password for some reason (e.g. forgetting password). For concerns of security this feature is only applicable for direct connection to the console port of the switch and the administrators only has 5 seconds during which they can input a specific key (shift+6) after boot up procedure is complete(i.e. when the username prompt or command prompt is shown).

When the specific key is inputted, user can enter reset configuration mode. In this mode, user can use the command **password-recovery** to

(1)Update the configuration for user account: update new password for existed user or add a user account.

(2)Force AAA module to switch the user authentication for console type to local authentication in case fail to connect the remove AAA server.

A series of prompt message will guide user to complete the Password Recovery procedure. User could answer "yes" to update the passwords or authentication function; answer "no" to skip it.

When Password Recovery procedure is done, user could use "logout" command to exit the reset configuration mode. After that, user could login system again with the new password.

Prompt Message

Prompt Message at screen	Description
Exceed the max number of user account.	If the table of user accounts is full, the user canot add a new user and can only update the password for an exsisting user.

Example This example shows how to using password recovery

```
Switch(reset-config)# password-recovery
This command will guide you to do the password recovery procedure.
Do you want to update the user account (y/n) [n]?y
Please input user account: alex
Please input user password:
Do you want to update privilege password (y/n) [n]?y
Please input privilege password:
Do you want to force switching authentication function of AAA modules to do
local authentication for console type (y/n) [n]?y

Switch(reset-config)# logout
User Access Verification

Username: alex
Password:

                  Chassis-based High-Speed Switch
                 Command Line Interface

                             Firmware: 1.00.014
          Copyright (c) 2010 D-Link Corporation. All rights reserved.
DGS-6600:15#
```

This example shows the situation when user account is full.

User could use **show username** command to find the existent user account, when the number of user account reaches to maximum and the user wants to add a new account, the error message will be prompt.

```
Switch(reset-config)#show username
Password Encryption : Disabled
Username                         Access Level Password
  Encrypted
--------------------------------------------------------------------------
-----
aaa                              15           123456
bbb                              15           123456
ccc                              15           123456
ddd                              15           123456

Total Entries: 4
Switch(reset-config)#
Switch(reset-config)# password-recovery
This command will guide you to do the password recovery procedure.
Do you want to update the user account (y/n) [n]?y
Please input user account: apple
Please input user password:
Exceed the max number of user account
Switch(reset-config)#
```

This example shows how to verify the configuration:

```
Switch(reset-config)#show username
Password Encryption : Disabled
Username                        Access Level Password
  Encrypted
--------------------------------------------------------------------------
-----
alex                            15           123456

Total Entries: 1
Switch(reset-config)#


Switch reset-config)#show aaa
Console Session:
  Login  authentication:
    Local Authentication: yes
  Enable authentication:
    Local Authentication: yes

Telnet Session:
  Login  authentication:
    Local Authentication: yes
  Enable authentication:
    Local Authentication: yes

Ssh Session:
  Login  authentication:
    Local Authentication: yes
  Enable authentication:
    Local Authentication: yes

Http Session:
  Login  authentication:
    Local Authentication: yes
  Enable authentication:
    Local Authentication: yes
Switch(reset-config)#
```

password encryption

Use the **password encryption** command to enable encryption of the password defined by both:

- the username command

  - and -

- the enable command

before they are stored in the configuration file. Using the no command will disable the encryption.

password encryption

no password encryption

Syntax None

Default Disabled

Command Mode Global configuration at privilege level 15

Usage Guideline The user account configuration information will be stored in the configuration file, and can be applied to the system later.

If the password encryption is enabled, the password will be in encrypted form.

When password encryption is disabled, and the user specifies the password in plain text form, the password will be in plain text form. However, if the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enable password encryption command, the password will stay in the encrypted form. Once in the encrypted form it cannot revert to plaintext.

Example The below example shows how to enable password encryption.

```
Switch(config)# password encrypt
```

Verify the settings by entering the **show system protocol-state** command.

periodic

Use the **periodic** command to specify the period of time to be covered in a time range profile.

periodic { daily *HH:MM* to *HH:MM* **| monthly** *DATE HH:MM* to *[DATE] HH:MM* **| weekly** *WEEKLY-DAY HH:MM* to **[** *WEEKLY-DAY* **]** *HH:MM* **}**

Syntax Description	
daily *HH:MM to HH:MM*	Specifies the time of day with an hour:minute format *HH:MM*, using a 24-hour clock (for example, 14:30). The first *HH:MM* time entered must be earlier than the second *HH:MM.* Note: The HH range is 00 ~ 23; The MM range is 00 ~ 59.
weekly *WEEKLY-DAY HH:MM* to **[** *WEEKLY-DAY* **]** *HH:MM*	Specifies the day of the week and time of day in the format *day HH:MM*, where the day of the week name is used i.e. monday, tuesday, wednesday, thursday, friday, saturday, and sunday. If the ending day of the week is the same as the starting day of the week, it can be omitted (then it is the same as the daily format).
monthly *DATE HH:MM* to **[** *DATE* **]** *HH:MM*	Specifies the numeric date, from 1 to 31, and the time of day, in the format *DATE HH:MM*. If the day does not exist on the calender, the specified time period will be skipped. For example, since April has only 30 days an entry such as “April 31” will be ignored.

Default None

Command Mode Time-range configuration

Usage Guideline Up to 6 periods can be specified in the same profile. A new period entry can partially overlap an older existing one. If a new period's starting and the ending time are identical to a previous entry, a warning message is displayed and the configuration will not be accepted.

Note: To remove an individual period entry delete the time-range and then create a new time-range to which the correct period entry can be added.

Example This example shows how to make a time-range which includes the periods daily 09:00 to 12:00, 00:00 Saturday to 23:59 Sunday, and 19:00 of the 1st day to 17:00 of the 2nd day of every month.

```
Switch(config)#time-range rdtime
Switch(config-time-range)#periodic daily 9:00 to 12:00
Switch(config-time-range)#periodic weekly saturday 00:00 to sunday 23:59
Switch(config-time-range)#periodic monthly 1 19:00 to 2 17:00
Switch(config)#end
```

Verify the settings by entering the **show time-range** command.

permit | deny (ip access-list)

Use the **permit** command to define the rule for packets to be access based on their IP header information. Use the **no permit** command to remove a permit entry. Use the **deny** command to add a deny entry. Use the **no deny** command to remove a deny entry.

{ permit | deny } tcp { any | host *SRC-IP-ADDR* **|** *SRC-IP-ADDR MASK* **} [** *OPERATOR PORT* **] { any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR MASK* **} [** *OPERATOR PORT* **] [precedence** *PRECEDENCE* **| tos** *TOS* **|dscp DSCP] [time-range** *PROFILE-NAME* **] [priority** *PRIORITY* **]**

{ permit | deny } udp { any | host *SRC-IP-ADDR* **|** *SRC-IP-ADDR MASK* **} [** *OPERATOR PORT* **] { any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR MASK* **} [** *OPERATOR PORT* **] [precedence** *PRECEDENCE* **| tos** *TOS* **|dscp** *DSCP* **] [time-range** *PROFILE-NAME* **] [priority** *PRIORITY* **]**

{ permit | deny } [gre | esp | eigrp | icmp | igmp | ospf | pim | vrrp | protocol-id *PROTOCOL-ID* **] { any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR MASK* **} { any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR MASK* **} [precedence** *PRECEDENCE* **| tos** *TOS* **| dscp** *DSCP***] [time-range** *PROFILE-NAME* **] [priority** *PRIORITY* **]**

no { permit | deny } tcp { any | host *SRC-IP-ADDR* **|** *SRC-IP-ADDR MASK***} [***OPERATOR PORT* **] { any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR MASK***} [** *OPERATOR PORT* **] [precedence** *PRECEDENCE* **| tos** *TOS* **| dscp** *DSCP* **] [time-range]**

no { permit | deny} udp { any | host *SRC-IP-ADDR* **|** *SRC-IP-ADDR MASK* **} [** *OPERATOR PORT* **] { any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR MASK* **} [** *OPERATOR PORT* **] [precedence** *PRECEDENCE* **| tos** *TOS* **| dscp** *DSCP* **] [time-range]**

no { permit | deny } [gre | esp | eigrp | icmp | igmp | ospf | pim | vrrp | protocol-id *PROTOCOL-ID* **] {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR MASK* **} { any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR MASK* **} [precedence** *PRECEDENCE* **| tos** *TOS* **| dscp** *DSCP* **] [time-range]**

Syntax Description	
any	Means any source IP address or any destination IP address.
host *SRC-IP-ADDR*	Specifies a specific source IP address.
SRC-IP-ADDR MASK	Specifies a group of source IP addresses by using mask.
host *DST-IP-ADDR*	Specifies a specific destination IP address.
DST-IP-ADDR MASK	Specifies a group of destination IP addresses by using mask.
precedence *PRECEDENCE*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7.
dscp *DSCP*	(Optional) Specifies the Differentiated Services Control pointer (DSCP) value, as specified by a number from 0 to 63.
tos *TOS*	(Optional) Packets can be filtered by the type of service level, as specified by a number from 0 to 255.

OPERATOR PORT	(Optional) Compares source or destination port. *OPERATOR* can be **lt** (less than, match on a lower port number), **gt** (greater than, match on a greater port), **eq** (equal, match on a specific port). The *PORT* argument can be the L4 TCP/UDP source or destination port, as specified by a number from 0 to 65535.
time-range *PROFILE-NAME*	(Optional) Specifies the name of time-period profile for activation of the access-list. In the no form of the commands, this option, time-range (without *PROFILE-NAME*),removes the setting of the active timer-period, rather than removing the whole entry.
PRIORITY	The range is 1 to 65535. The less number represents for the better priority. It represents the rule sequence number.
tcp, udp, icmp, igmp, gre, esp, eigrp, ospf, pim, vrrp	Layer 4 protocols.
PROTOCOL-ID	Protocol ID refers to the protocol field in the IP header, as specified by a number from 0 to 65535.

Default None

Command Mode ip access-list configuration or ip extended access-list configuration

Usage Guideline An interface can have only one MAC access list, one IP access list and one IPv6 access list applied to it.

The time range profile must be created before it can be specified in the statement. Otherwise an error message will be displayed.

An error message will be displayed if the maximum number defined by the system is exceeded.

All the configurable arguments (excluding time-range and priority) can be used to differentiate one from another. These arguments are called differentiated arguments. To remove an entry with the no form of this command, it is necessary to specify the entry using the same value of all differentiating arguments that have been specified (includes all optional parameters except time-range and priority).

To update the time-range or priority, specify the entry with the same value of all differentiating arguments, that have been configured, and the update value for the time-range or priority.

The priority value must be unique in the domain of an access-list. If a priority value that is already present is entered, an error message will be shown.

Example This example shows create three entries for an ip access-list, named "Strict-Control". The three entries are: tcp packets destined to network 10.20.0.0/16, tcp packets destined to host 10.100.1.2 and all icmp packets.

```
Switch(config)# ip access-list extended Strict-Control
Switch(config-ip-ext-acl)# permit tcp any 10.20.0.0 255.255.0.0
Switch(config-ip-ext-acl)# permit tcp any host 10.100.1.2
Switch(config-ip-ext-acl)# permit icmp any any
Switch(config-ip-ext-acl)# exit
```

Verify the settings by entering the **show access-list** command.

permit | deny (ipv6 access list)

Use the **permit** command to add an entry to the IPv6 access-list. Use the **no permit** command to remove a permit entry from the IPv6 access-list. Use the **deny** command to add a deny entry to the IPv6 access-list. Use the **no deny** command to remove a deny entry from the IPv6 access-list.

{ permit | deny } {tcp | udp} { any | host SRC-IPV6-ADDR | SRC-IPV6-ADDR MASK } [OPERATOR PORT] { **any | host** DST-IPV6-ADDR | DST-IPV6-ADDR MASK } [OPERATOR PORT] **[traffic-class** TRAFFIC-CLASS] [**time-range** PROFILE-NAME] [**priority** PRIORITY]

{ permit | deny } [icmpv6 | ospfv3 | nextheader NEXTHEADER] { **any | host** SRC-IPV6-ADDR | SRC-IPV6-ADDR MASK } { **any | host** DST-IPV6-ADDR | DST-IPV6-ADDR MASK } [**traffic-class** TRAFFIC-CLASS] [**time-range** PROFILE-NAME] [**priority** PRIORITY]

no { permit | deny } {tcp | udp} { any | host SRC-IPV6-ADDR | SRC-IPV6-ADDR MASK } [OPERATOR PORT] { **any | host** DST-IPV6-ADDR | DST-IPV6-ADDR MASK } [OPERATOR PORT] **[traffic-class** TRAFFIC-CLASS] **[time-range]**

no { permit | deny} [icmpv6 | ospfv3 |nextheader NEXTHEADER] { **any | host** SRC-IPV6-ADDR | SRC-IPV6-ADDR MASK} { **any | host** DST-IPV6-ADDR | DST-IPV6-ADDR MASK} **[traffic-class** TRAFFIC-CLASS] **[time-range]**

Syntax Description	
Any	An abbreviation for the IPv6 prefix ::/0
host *SRC-IPV6-ADDR*	Specifies a specific source IPv6 address.
SRC-IPV6-ADDR MASK	Specifies a source IPv6 addresses by using a mask.
host *DST-IPV6-ADDR*	Specifies a specific destination IPv6 address.
DST-IPV6-ADDR MASK	Specifies a group of destination IPv6 addresses by using a mask.
tcp, udp, icmpv6, ospfv3	L4 protocol type of the next header in the IPv6 header.
nextheader *NEXTHEADER*	The value of the nextheader in IPv6 header. The range is from 0 to 255
traffic-class *TRAFFIC-CLASS*	(Optional) Specifies the traffic class value in IPv6 header. The acceptable range is from 0 to 255.
OPERATOR PORT	(Optional) Compares source or destination port. OPERATOR can be **lt** (less than, match on a lower port number), **gt** (greater than, match on a greater port), **eq** (equal, match on a specific port). The PORT argument can be the L4 TCP/UDP source or destination port. The acceptable range is from 0 to 65535 for **eq** operator. The acceptable range is from 0 to 65534 for **gt** operator. The acceptable range is from 1 to 65534 for **lt** operator
time-range	(Optional) Specifies the name of time-period profile for activation the access-list.

Syntax Description	
PROFILE-NAME	Used with the no form of the commands, this option, time-range (without PROFILE-NAME), means to remove the setting of an active timer-period, rather than remove the whole entry.
PRIORITY	The range is 1 to 65535. The lower the number represents a better priority. It is used as the rule sequence number.

Default None

Command Mode IPv6 access-list extended configuration

Usage Guideline The time range profile needs to be created before it can be specified in the statement. Otherwise an error message will be displayed.

All the configurable arguments (time-range and priority are excluded) can be used to differentiate one from another. These arguments are called differentiated arguments. To remove an entry, in the no form of this command, specify the entry with the same value of all differentiating arguments specified prior (includes all optional parameters but the time-range and priority are excluded).

Tto update the time-range or priority, specify the entry with the same value of all differentiating arguments, which are configured, and the update value for time-range or priority.

The priority value must be unique in the domain of an access-list. If a priority value entered is already present, an error message will be shown.

Example This example shows create three entries for an ipv6 extended access-list, named "ipv6-control". The three entries are: permit tcp packets destined to network ff02::0:2/16, permit tcp packets destined to host ff02::1:2 and permit all icmp packets.

```
Switch(config)# ipv6 access-list extended ipv6-control
Switch(config-ipv6-ext-acl)#permit tcp any ff02::0:2 ffff::
Switch(config-ipv6-ext-acl)#permit tcp any host ff02::1:2
Switch(config-ipv6-ext-acl)#permit icmpv6 any any
Switch(config-ipv6-ext-acl)# exit
```

Verify the settings by entering the **show access-list** command.

permit | deny (mac access-list)

Use the **permit** command to define the rule for packets to be based on their MAC address. Use the **deny** command to define the rule for packets that are to be denied. Use the **no permit** command to remove a permit entry, and use the **no deny** command to remove a deny entry.

{ permit | deny } { any | host *SRC-MAC-ADDR* **|** *SRC-MAC-ADDR MASK* **} { any | host** *DST-MAC-ADDR* **|** *DST-MAC-ADDR MASK* **} [ethernet-type** *TYPE* **| llc dsap** *DSAP* **ssap** *SSAP* **cntl** *CNTL* **] [dot1p** *PRIORITY-TAG* **] [VLAN** *VLAN-ID* **] [time-range** *PROFILE-NAME* **] [priority** *PRIORITY* **]**

no { permit | deny } { any | host *SRC-MAC-ADDR* **|** *SRC-MAC-ADDR MASK* **} { any | host** *DST-MAC-ADDR* **|** *DST-MAC-ADDR MASK* **} [ethernet-type***TYPE* **| llc dsap** *DSAP* **ssap** *SSAP* **cntl** *CNTL* **] [dot1p** *PRIORITY-TAG* **] [VLAN** *VLAN-ID* **] [time-range]**

Syntax Description	
any	Specifies any source MAC address or any destination MAC address.
host *SRC-MAC-ADDR*	Specifies a specific source MAC address.
SRC-MAC-ADDR MASK	Specifies a group of source MAC addresses using a mask.
host *DST-MAC-ADDR*	Specifies a specific destination MAC address.
DST-MAC-ADDR MASK	Specifies a group of destination MAC addresses by using mask.
ethernet-type*TYPE*	(Optional) Specifies that the protocol type for the Ethernet_II packet or a SNAP packet by specifying the Ethernet type value which is a number from 0 to 65535.
llc dsap *DSAP* **ssap** *SSAP* **cntl** *CNTL*	(Optional) Specifies the protocol type for the LLC packet by specifying the DSAP, SSAP and CONTROL number which is a number from 0 to 255.
dot1p *PRIORITY-TAG*	(Optional) Priority tag in value of 0~7.
VLAN *VLAN-ID*	(Optional) Specifies the VLAN ID which a number from 1 to 4094.
time-range *PROFILE-NAME*	(Optional) Specifies the name of a time-period profile for activation of the access-list. With the no form of this command, this option, time-range (without *PROFILE-NAME*), removes the setting of an active timer-period, rather than removing the whole entry.
priority *PRIORITY*	(Optional) Access entry priority range is 1 to 65535 where the lower value represents higher priority for the sequence number. If no priority is specified, the system automatically assigns it with a priority that is 10 greater than the largest sequence in that access list and places it at the end of the list.

Default

If the priority is not specified, the system assigns it with a priority value 10 or greater than the largest sequence in that access list and it is placed at the end of the list.

If the priority is manually assigned, it is better to have a reserved interval for a future higher priority entry. Otherwise the system attempts to insert an entry with a higher priority.

Command Mode MAC access-list extended configuration

Usage Guideline The time-range profile must be created before it can be specified in the statement. Otherwise, an error message will be displayed.

Multiple entries can be added to the list; use **permit** for one entry and use **deny** for the other entry.

Different **permit** and **deny** commands can match different fields available for setting.

The priority can be directly updated by specifying the command with the value for all other parameters except time-range & priority.

All the configurable arguments (**time-range** and **priority** are excluded) can be used to differentiate one from another. These arguments are called differentiating arguments. To remove an entry, using the **no** form of this command, specify the entry with same value of all differentiating arguments specified (includes all optional parameters but **time-range** and **priority** are excluded). The **time-range** option in **no** form of this command means to remove the time-range association from this entry.

To update the time-range or priority, specify the entry with the same value of all differentiating arguments, which are configured, and the update value for time-range or priority.

The priority value must be unique in the domain of an access-list. If r a priority value is entered that is already present, an error message will be shown.

When the time-range is not specified, the statement will be always effective.

Example This example shows how to configure access entries in the profile daily-profile to allow two sets of source MAC addresses. Others are denied due to default implicit deny rule.

```
Switch(config)# mac access-list extended daily-profile
Switch(config-mac-ext-acl)# permit 00:80:33:00:00:00 ff:ff:ff:00:00:00 any
Switch(config-mac-ext-acl)#permit  00:f4:57:00:00:00 ff:ff:ff:00:00:00 any
Switch(config-mac-ext-acl)# exit
Switch(config)#
```

Verify the settings by entering the show **show access-list** command.

ping

Use ping to diagnose basic network connectivity.

ping [*OPTIONS***] {** *IP-ADDRESS* **|** *IPV6-ADDRESS* **}**

Syntax Description	
OPTIONS	(Optional) The option can be any combination of the following parameters: -A Adapt to return interval of packets. That is to send packets at approximately the rate at which they are received. -c *COUNT* Stop after sending count ECHO_RESPONSE packets. -i *WAIT* Wait WAIT seconds between sending each packet. Default is to wait one second between each packet. This option is incompatible with -A option and it will be ignored when it is along with -A option. -**Q** *TOS* Set Quality of Service on ICMP data grams. -**s** *PACKETSIZE* Specifies the number of data bytes to be sent. Default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data. It does not include any VLAN or IEEE802.1Q tag length. -**w** *N* Stop ping after N seconds. -**W** *N* When waiting for a response, time out after N seconds. If N is not specified, the default is one second.
IP-ADDRESS	IPv4 address in dot notation (a.b.c.d) of the destination host.
IPV6-ADDRESS	IPv6 address of the destination host.

Default

-s: 56 bytes

-c: 5 count packets

-i: 1 second

-Q: 0 TOS

-w: 0 (Don't stop)

-W: 1 second

Command Mode Management interface configuration or User EXEC

Usage Guideline The ping command sends an echo request packet to an address, and then awaits a reply. Ping output can help to evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

Note : The specified "OPTIONS" can be any combination of the parameters but the parameters must be specified in the alphabetical order and the upper case is ahead of the lower case. For example, e the following sequences cannot be used with the specified parameters: "ping -c COUNT -Q TOS -A 10.90.90.90". The correct usage is: "ping -A -Q TOS -c COUNT 10.90.90.90".

Examples This example shows how to ping the host with IP address 172.50.71.123.

```
Switch# ping 172.50.71.123
PING 172.50.71.123 (172.50.71.123): 56(84) data bytes
64 bytes from 172.50.71.123, icmp_seq=1 ttl=128 time=0.226 ms
64 bytes from 172.50.71.123, icmp_seq=2 ttl=128 time=0.184 ms
--- 172.50.71.123 ping statistics ---
packets transmitted = 2, received = 2 , packet loss = 0 (0%)
round trip times min/avg/max/mdev = 0.184/0.205/0.226/0.021 ms
Switch#
```

This example shows how to ping the host with IPv6 address 2001:e10:5c00:2::101:150.

```
Switch# ping 2001:e10:5c00:2::101:150
PING 2001:e10:5c00:2::101:150 (2001:e10:5c00:2::101:150):56(104) data bytes
64 bytes from 2001:e10:5c00:2::101:150, icmp_seq=1 ttl=128 time=92.1 ms
64 bytes from 2001:e10:5c00:2::101:150, icmp_seq=2 ttl=128 time=0.766 ms
64 bytes from 2001:e10:5c00:2::101:150, icmp_seq=3 ttl=128 time=0.781 ms
64 bytes from 2001:e10:5c00:2::101:150, icmp_seq=4 ttl=128 time=0.774 ms
64 bytes from 2001:e10:5c00:2::101:150, icmp_seq=5 ttl=128 time=0.760 ms
--- 2001:e10:5c00:2::101:150 ping statistics ---
packets transmitted=5, received=5, packet loss=0 (0%)
round trip times min/avg/max/mdev= 0.760/19.040/92.120/36.540 ms
Switch#
```

poe port priority

Use this command to configure the priority of power-sourcing for ports. Use the no poe port priority command to return to the default settings.

poe port priority {1st | 2nd | 3rd}

no poe port priority

Syntax Description	
{1st | 2nd | 3rd}	The 1st, 2nd and 3rd port priority. The lower number has the higher priority

Default The default priority for all of ports is the lowest one (3rd).

Command Mode Interface configuration

Usage Guideline PoE supervisor system will calculate the available power which is called the power budget when system initializes. Once the system is running out of power budget, cannot provide enough power to the connected PDs. Supervisor system will reallocate the power for all active PoE ports. The port with higher priority will get power first. Then there is a possibility - low priority port power could be cut off because of a new higher priority port is connected with a PD and power budget is limited.

The relinquishment of PoE port power can cross unit by the management of PoE supervisor system that means if there are multiple ports have been assigned with same priority, then these ports will be powered off when system power is going to be insufficient after inserting a PD at higher priority port. In the condition of multiple ports with the same priority, the port ID with less number take precedence.

Example This example shows how to configure PoE port priority at port eth3.1 with the first priority.

```
Switch(config)# interface eth3.1
Switch(config-if)#poe port priority 1st
Switch(config-if)#end
Switch(config)#
Switch#
```

poe port description

Use the poe port description command to configure the PoE port specific description. Use no form of this command to clear the existed description.

poe port description TEXT

no poe port description

Syntax Description	
description	String that describes the PoE ports specific information. The maximum length is 128 characters. The syntax is a general string that allows space.

Default The default value of this description is a zero-length string.

Command Mode Interface configuration.

Usage Guideline This command could be used to configure a per-port description to indicate the type of powered device that is connected to the port.

Example This example shows how to configure the PoE port description.

```
Switch(config)# interface eth3.1
Switch(config-if)# poe port description For VOIP usage
```

poe service-policy

Use the command to configure power service policy for whole system's usage under power shortage condition.

poe service-policy { preemptive | non-preemptive }

Syntax Description	
non-preemptive	The power will not be provided to the new PD connected port regardless of port priority setting if the unit enters into critical section.
preemptive	If there are ports that have been provided with power with a lower priority than the new PD connected port and there comes power shortage, the connected PD port with the lowest priority will be disconnected. This process will be performed continuously until enough power is released for the new connected higher priority port or no available PD port can be disconnected.

Default non-preemptive.

Command Mode Global configuration.

Usage Guideline The PoE system has a limited power watts referred as power budget. Once the used power almost reaches the power budget limit, this condition is referred as power critical section.

The service policy is used to determine the power service behavior as PoE power system enters the critical section. If the PoE system is configured with non-preemptive, no additional port can be serviced with power once the PoE system enter critical section. However if the preemptive mode is configured, additional port can be powered up with a cross-unit power management as long as its priority is higher than all other serviced ports.

In the situation of containing units which is not PoE capable in the system, there will be a message displayed for reminding those units will not take effect with this command.

Example This example shows how to configure POE system power service policy as non-preemptive mode.

```
Switch(config)# poe service-policy non-preemptive
```

You can verify your settings by entering the **show poe power system** command.

poe power-inline

Use this command to configure the power management mode on the Power over Ethernet (PoE) ports.

poe power-inline { auto | never | static [max MAX-WATTAGE **] } [time-range] [**PROFILE-NAME **]**

Syntax Description	
auto	Enable powered-device detection. If enough power is available, automatically allocate power to the PoE port after device detection based on IEEE802.3af.
never	Disable device detection, and disable power to the port.
static	Disable powered device detection. The power quantity which allowed to the port is configured by user manually.
max MAX-WATTAGE	(Optional) Limit the power allowed on the port. The unit is milli-watt (mW). The range is 4000 to 17000 mW. If no value is specified, the maximum is allowed.
time-range PROFILE-NAME	(Optional) Specifies the name of time-range profile associated with the per-port power-inline configuration delineating its activation period. If no PROFILE-NAME is specified, that means to remove the time-range binding of the port instead of disable the PoE functionality.

Default

The default mode is **never** (disabled).

The default power threshold value in auto mode is 16.2W, 4.2W, 7.4W and 16.2W for class-0, class-1, class-2 and class-3 respectively.

The default maximum power threshold in static mode is 17000 mW.

Command Mode

Interface configuration.

Usage Guideline

This command is supported only on PoE-capable ports. If you enter this command on a port that does not support PoE, an error message appears to indicate the corresponding message.

Under the static mode, if the powered device requesting more power than the maximum power threshold, the switch removes power from the port, and the port state will be set to "faulty" to indicate the error If the powered-device IEEE class maximum is greater than the maximum wattage, the switch does not power the device. The power is reclaimed into the global power budget.

In auto mode configuration, the power threshold is configured by the PoE chip itself, and the value will be 16.2W, 4.2W, 7.4W and 16.2W for class-0, class-1, class-2 and class-3 respectively. These threshold value will also used as the allocated power for that port.

The maximum power threshold value in static mode is designed as 17W. The reason is, the actual voltage which PSE side output and the actual current which PD drains will both have the tolerance inaccuracy. Generally, the tolerance is 5%. Thought, in the worst case, the actual power which PSE needs to offer will be 1.1025(1.05*1.05) times of maximum power consumption (15.4W) defined in

IEEE802.3af, it will be 16.9785W. This design is also for the better conformance of DGS-6600's PoE functionality. But we strongly recommend using 15.4W as the maximum power threshold in static mode. If PD only needs 15.4W, but the port is configured as maximum power threshold. That means PoE system will take 17W from system power budget and 1.6W will be wasted!

The time range function could be also applied on PoE with a per-port based methodology. Once a PoE port is combined with a time-range profile, it will only be activated with the time range which that profile specified. The time-range profile must be created before it is applied.

Example

This example shows how to enable detection of a powered device and to automatically power a PoE port for interface eth3.1-3.5.

```
Switch(config)# interface range eth3.1-3.5
Switch(config-if-range)# poe power-inline auto
```

The following is an example showing how to configure a PoE interface eth3.1, allows class 1 or a class 2 powered device under 7000mw:

```
Switch(config)# interface eth3.1
Switch(config-if)# poe power-inline static max 7000
```

This example shows how to disable powered-device detection and to not power a PoE port (eth3.1).

```
Switch(config)# interface eth3.1
Switch(config-if)# poe power-inline never
```

This example shows how to combine a time-range profile "rd_time" with PoE interface eth3.1.

```
Switch(config)# interface eth3.1
Switch(config-if)# poe power-inline auto time-range rd_time
```

You can verify your settings by entering the **poe power inline status** command.

police

To configure traffic policing using single rate, use the police command in policy-map class configuration mode. To remove traffic policing from the configuration, use the no form of this command.

police *BPS [BURST-NORMAL] [BURST-MAX]* **exceed-action** *ACTION* **[violate-action** *ACTION***]**

no police *BPS [BURST-NORMAL] [BURST-MAX]* **exceed-action** *ACTION* **[violate-action** *ACTION***]**

Syntax Description	
BPS	Average rate, in bits per second. min: 64KB max:32G.
BURST-NORMAL	(Optional) Normal burst size in bytes. min:4KB max:16MB default:4KB. Unit is KB
BURST-MAX	(Optional) Maximum burst size, in bytes. Valid values are project dependent min:4KB max:16MB default:4KB. Unit is KB "police BPS BURST-NORMAL BURST-MAX exceed-action ACTION violate-action ACTION For the above case, the explicit BURST-NORMAL BURST-MAX values are used. "police BPS BURST-MAX exceed-action ACTION violate-action ACTION For the above case, the default BURST-NORMAL and explicit BURST-MAX values are used. "police BPS exceed-action ACTION violate-action ACTION For the above case, the default BURST-NORMAL and default BURST-MAX values are used. "police BPS BURST-NORMAL exceed-action ACTION For the above case, the explicit BURST-NORMAL and explicit BURST-MAX values are used.
exceed-action	Specifies action to take on packets that exceed the rate limit.
violate-action	(Optional) Specifies action to take on packets that violate the normal and maximum burst sizes.

Syntax Description	
ACTION	Action to take on packets. Specifies one of the following keywords: "drop-Drops the packet. "set-dscp-transmit value-Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. "transmit-Transmits the packet. The packet is not altered.

Default None

Command Mode Policy-map class configuration

Usage Guideline Use the police command to drop the packet or mark the packet with different quality of service (QoS) values based on conformance to the service agreement.

As a packet arrives at a port, the packet will be initialized with a color. This color will be used in control of congestion.

If the policer is operated in color blind mode, the packet is re-colored and the actions are taken based on the policer metering result.

If the policer is operated in color aware mode, the packet is re-colored and the actions are taken based on the policer metering result and the initial color of the packet.

The actions configured by the set command for the traffic class will be applied to the conforming packet. They will not be applied to the exceeding packet and the violating packets.

Note: Either one of police command and police cir command can be activated for the refereed traffic class. The latter command will overwrite the previous policer command setting within the same traffic class.

The following example show the precedence between **police** command and **police cir** commands: create a policy-map, police-map1 and have a traffic class, class-movie with single rate police (police command).

```
Switch(config)# policy-map police-map1
Switch(config-pmap)# class class-movie
Switch(config-pmap-c)# police 8000 1000 exceed-action drop
Switch(config-pmap-c)#exit
Switch(config-pmap)# exit
Switch(config)#
```

Later it is realized that a two rate police should be applied to class-movie traffic and a two rate police (police cir command) is added. The newer police cir command will overwrite the previous police command setting.

```
Switch(config)# policy-map police-map1
Switch(config-pmap)# class class-movie
Switch(config-pmap-c)# police cir 8000 pir 1000 exceed-action drop violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

Specifying Multiple Actions

The police command allows to specify actions for different policing result. When specifying multiple policing actions, contradictory actions, such as violate-action transmit and exceed-action drop, cannot be specified.

Using the Police Command with the Traffic Policing Feature

The Traffic Policing feature works with a token bucket algorithm. Two types of token bucket algorithms are available: a one-token bucket algorithm and a two-token bucket algorithm. A single-token bucket system is used when the violate-action option is not specified, and a two-token bucket system is used when the violate-action option is specified.

The following are explanations of how the token bucket algorithms work.

Token Bucket Algorithm with One Token Bucket

The one-token bucket algorithm is used when the violate-action option is not specified in the police command CLI. The conform bucket is initially set to the full size (the full size is the number of bytes specified as the normal burst size).

When a packet of a given size (for example, "B" bytes) arrives at specific time (time "T"), the following actions occur:

"Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current time is T, the bucket is updated with (T - T1) worth of bits based on the token arrival rate. The token arrival rate is calculated as follows: (time between packets (which is equal to T - T1) * policer rate)/8 bytes. The policer rate here is average rate (BPS).

"If the number of bytes in the conform bucket is greater than or equal to the packet size, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is completed for the packet.

"If the number of bytes in the conform bucket (minus the packet size to be limited) is fewer than B, the exceed action is taken.

Token Bucket Algorithm with Two Token Buckets

The two-token bucket algorithm is used when the violate-action option is specified in the police command. The conform bucket is initially full (the full size

is the number of bytes specified as the normal burst size). The exceed bucket is initially full (the full exceed bucket size is the number of bytes specified in the maximum burst size). The tokens for both the conform and exceed token buckets are updated based on the token arrival rate, or committed information rate (CIR).

When a packet of given size (for example, "B" bytes) arrives at specific time (time "T") the following actions occur:

"Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current arrival of the packet is at T, the bucket is updated with T -T1 worth of bits based on the token arrival rate. The refill tokens are placed in the conform bucket. If the tokens overflow the conform bucket, the overflow tokens are placed in the exceed bucket.

The token arrival rate is calculated as follows:

(time between packets (which is equal to T-T1) * policer rate)/8 bytes. The policer rate here is average rate (BPS).

"If the number of bytes in the conform bucket is greater than or equal to B, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is taken. The exceed bucket is unaffected in this scenario.

"If the number of bytes in the conform bucket is less than B, the excess token bucket is checked for bytes by the packet. If the number of bytes in the exceed bucket is greater than or equal to B, the exceed action is taken and B bytes are removed from the exceed token bucket. No bytes are removed from the conform bucket.

"If the number bytes in the exceed bucket is fewer than B, the packet violates the rate and the violate action is taken. The action is complete for the packet.

Example

The following example shows how to define a traffic class (using the class-map command) and associate the policy with the match criteria for the traffic class in a policy map (using the policy-map command). The service-policy command is then used to attach this service policy to the interface.

In this particular example, traffic policing is configured with an average rate at 8000 bits per second and the normal burst size at 1000 bytes for all packets ingress at eth 3.1:

```
Switch(config)# class-map access-match
Switch(config-cmap)# match access-list acl_rd
Switch(config-cmap)# exit
Switch(config)# policy-map police-setting
Switch(config-pmap)# class access-match
Switch(config-pmap-c)# police 8000 1000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface eth3.1
Switch(config-if)# service-policy police-setting
```

Verify the settings by entering the **show policy-map** command.

police aggregate

To configure a named aggregate policer as the policy for a traffic class in a policy map, use police aggregate command in the policy map class configuration mode. To delete the name aggregate policer from class policy, use the no form of this command.

police aggregate *NAME*

no police aggregate *NAME*

Syntax Description	
NAME	Specifies a previously defined aggregate policer name as the aggregate policer for a traffic class. Up to 32 characters are allowed.

Default None

Command Mode Policy map class configuration

Usage Guideline Use the qos aggregate-policer command in global configuration mode to create a named aggregate policer, and then use the police aggregate command in the policy-map class configuration mode to configure the named aggregate policer as the policy for a traffic class. A named aggregate policer cannot be referred from different policy map.

Example This example shows how to configure a named aggregate policer parameters and apply the policer to multiple classes in a policy map: An aggregate policer with single rate policing named agg_policer1 is created. This policer is configured as the policy for traffic class class1, class2, and class3.

```
Switch(config)# qos aggregate-policer agg_policer1 64 128 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
```

Verify the settings by entering the **show policy-map** command.

police cir

To configure traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR), use the police cir command in policy-map class configuration mode. To remove two-rate traffic policing from the configuration, use the no form of this command

police cir *CIR* **[bc** *CONFORM-BURST***] pir** *PIR* **[be** *PEAK-BURST***] [exceed-action** *ACTION* **[violate-action** *ACTION***]]**

no police cir *CIR* **[bc** *CONFORM-BURST***] pir** *PIR* **[be** *PEAK-BURST***] [exceed-action** *ACTION* **[violate-action** *ACTION***]]**

Syntax Description	
CIR	Specifies the committed information rate in bits per second. The committed packet rate is the first token bucket for the two-rate metering. min: 64KB max:32GB
PIR	Specifies the peak information rate in bits per second. The peak information rate is the second token bucket for the two-rate metering. min: 64KB max:32GB
CONFORM-BURST	Specifies the burst size for the first token bucket in bytes. Valid values are project dependent. min:4KB max:16MB default:4KB
PEAK-BURST	Specifies the burst size for the second token bucket in bytes. Valid values are project dependent. min:4KB max:16MB default:4KB
exceed-action	(Optional) Specifies the action to take for those packets that conform to PIR but not to CIR. It is referred as yellow color traffic.
violate-action	(Optional) Specifies the action to take for those packets that did not conform to both CIR and PIR. It is referred as red color traffic.
ACTION	The actions can be **drop** - Packets will be dropped. **set-dscp-transmit** VALUE - Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. **transmit** - Transmits the packet. The packet is not altered.

Default Disabled

exceed-action: drop

violate-action: equals **exceed-action**

Command Mode Policy map class configuration

Usage Guideline As a packet arrives at a port, the packet will be initialized with a color. This color will be used in control of congestion.

If the policer is operated in color blind mode, the packet is re-colored and the actions are taken based on the policer metering result.

If the policer is operated in color aware mode, the packet is re-colored and the actions are taken based on the policer metering result and the initial color of the packet.

The actions configured by the set command for the traffic class will be applied to the conforming packet. They will not be applied to the exceeding packet and the violating packet.

Note: Either one of police command and police cir command can be activated for the refereed traffic class. The latter command will overwrite the previous policer command setting within the same traffic class.

The following example show the precedence between police and police cir comands: create a policy-map, police-map1 and have a traffic class class-movie with a two rate policer (police cir command).

```
Switch(config)# policy-map police-map1
Switch(config-pmap)# class class-movie
Switch(config-pmap-c)# police cir 8000 pir 1000 exceed-action drop violate-
action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

Later it is realized that a single rate policer should be applied to class-movie traffic and singe rate policer (police cir command) is added. The newer police command will overwrite the previous police cir command setting.

```
Switch(config)# policy-map police-map1
Switch(config-pmap)# class class-movie
Switch(config-pmap-c)# police 8000 1000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

Two-rate traffic policing uses two token buckets-Tc and Tp-for policing traffic at two independent rates. Note the following points about the two token buckets:

"The Tc token bucket is updated at the CIR value. The Tc token bucket can contain up to the confirm burst (Bc) value.

"The Tp token bucket is updated at the PIR value. The Tp token bucket can contain up to the peak burst (Be) value.

Updating Token Buckets

The following scenario illustrates how the token buckets are updated:

A packet of B bytes arrives at time t. The last packet arrived at time t1. The CIR and the PIR token buckets at time t are represented by Tc(t) and Tp(t), respectively. Using these values and in this scenario, the token buckets are updated as follows:

Tc(t) = min(CIR * (t-t1) + Tc(t1), Bc)

Tp(t) = min(PIR * (t-t1) + Tp(t1), Be)

Marking Traffic

The two-rate policer marks packets as either conforming, exceeding, or violating a specified rate. The following points (using a packet of B bytes) illustrate how a packet is marked:

"If B > Tp(t), the packet is marked as violating the specified rate.

"If B > Tc(t), the packet is marked as exceeding the specified rate, and the Tp(t) token bucket is updated as Tp(t) = Tp(t) - B.

Otherwise, the packet is marked as conforming to the specified rate, and both token buckets-Tc(t) and Tp(t)-are updated as follows:

Tp(t) = Tp(t) - B

Tc(t) = Tc(t) - B

Example

Example In the following example, two-rate traffic policing is configured on a class called police to limit traffic to an average committed rate of 64 kbps and a peak rate of 128 kbps, and the policy map named policy1 is attached to eth3.1.

```
Switch(config)# class-map police
Switch(config-cmap)# match access-list 101
Switch(config-cmap)# policy-map policy1
Switch(config-pmap)# class police
Switch(config-pmap-c)# police cir 64 bc 128 pir 128 be 256 exceed-action
drop violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface eth3.1
Switch(config-if)# service-policy policy1
Switch(config-if)# end
Switch# show policy-map policy1
Policy Map policy1
  Class police
   police tr-tcm cir 64 bc 128 pir 128 be 256
          exceed-action : drop
         violate-action : drop
Switch#
```

Verify the settings by entering the **show policy-map** command.

policy-map

To enter policy-map configuration mode and create or modify a policy map that can be attached to one or more interfaces as a service policy, use the policy-map command in global configuration mode. To delete a policy map, use the no form of this command.

policy-map *NAME*

no policy-map *NAME*

Syntax Description	
NAME	Name of the policy map. The name can be a maximum of 32 alphanumeric characters

Default None

Command Mode Global configuration

Usage Guideline Use the policy-map command to specify the name of the policy map to be created, or modified before policies are configured for classes whose match criteria are defined in a class map. The policy-map command enters policy-map configuration mode, in which the user can configure or modify the policy for the traffic class.

The user can configure class policies in a policy map only if the classes have match criteria defined for them. Use the class-map and match commands to configure the match criteria for a class. Because a maximum of 32 class maps is allowed, a policy map cannot contain more than 32 class policies.

A single policy map can be attached to more than one interface concurrently.

Policy maps contain traffic classes. Traffic classes contain one or more match commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application. Create as many traffic classes as needed.

Example The following example (on the next page) creates a policy map called policy and configures two class policies in that policy map. The class policy called class1 specifies policy for traffic that matches access control list (ACL) acl_rd. The

second class is the default class, named class-default to which packets that do not satisfy the defined classes are included.

```
Switch(config)# class-map class1
Switch(config-cmap)# match access-list acl_rd
Switch(config-cmap)# exit
Switch(config)# policy-map policy
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 46
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip dscp 00
Switch(config-pmap-c)# exit
```

Verify the settings by entering the **show policy-map** command

port-channel load-balance

Use port-channel load-balance to configure the load balance algorithm that the switch uses to distribute packets across ports in the same channel. To reset the load distribution to the default settings, use the no from of this command.

port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}

no port-channel load-balance

Syntax Description	
dst-ip	Indicates that the switch should examine the IP destination address.
dst-mac	Indicates that the switch should examine the MAC destination address.
src-dst-ip	Indicates that the switch should examine the IP source address and destination address.
src-dst-mac	Indicates that the switch should examine the MAC source and destination address.
src-ip	Indicates that the switch should examine the IP source address.
src-mac	Indicates that the switch should examine the MAC source address.

Default **src-dst-mac**

Command Mode Global configuration

Usage Guideline Use this command to specify the load balance algorithm. Only one algorithm can be specified.

Example This example shows how to configure load balance algorithm for src-ip:

```
Switch# configure terminal
Switch(config)#  port-channel load-balance src-ip
Switch(config)# end
```

Verify the settings by entering the **show channel-group load-balance** *EXEC* command.

power-saving

Use the power-saving command to enable "Power Saving" function in the device. And use the no form of this command to disable "Power Saving" function.

power-saving {phy}

no power-saving {phy}

Default Disabled

Command Mode Global configuration.

Usage Guideline The "power-saving" command can enable the "Power Saving" function on different hardware components. Currently, one component is supported: phy. Select the option "phy", it will set the PHY into "Power Saving" mode. The "no power-saving" command disables this function.

The "PHY Power Saving" function could be enabled or disabled per-system base. There are two operation modes: "low-power" mode and "normal" mode. When power saving is enabled, the chips automatically enter "low-power" mode if the signal from a copper link partner is lost. They will go to normal mode when a signal is detected.

If "PHY Power Saving" function is disabled, PHY will always be in normal mode no matter that the signal froma link partner is presented or not.

Example The following example shows how to enable/disable "Power Saving" function.

```
Switch(config)#power-saving
Switch(config)#
Switch(config)show power-saving

Power-saving status
===========================
phy power-saving:Enabled

Switch(config)#no power-saving
Switch(config)#show power-saving

Power-saving status
===========================
phy power-saving:Disabled
```

pvid VLAN-ID

Use the pvid interface configuration command to specify the native VLAN for the trunk or hybrid interface. Use default interface command to reset to default setting.

pvid *VLAN-ID*

default pvid

Syntax Description	
pvid *VLAN-ID*	Specifies the PVID for the trunk or hybrid interface.

Default **pvid** *VLAN-ID*: 1 (If the port is set to trunk/hybrid mode)

Command Mode Interface configuration

Usage Guideline The valid interfaces for this command are physical port or port-channel.

An interface can be specified with only one PVID. The succeeding command overwrites the previous command.

This command is used to change PVID of Trunk or Hybrid port. When an interface is Access mode, use the **access** VLAN command to change its PVID instead of this command.

This command does not affect the VLAN membership and the port's tag handling mode (Access, Hybrid or Trunk). Use the trunk allowed-VLAN or hybrid VLAN command to add the port to the VLAN by the requirement. The specified VLAN does not need to exist to make the command succeed.

Example This example shows how to set an interface port 4.1 as a hybrid interface with native VLAN 1000.

```
Switch(config)# interface eth4.1
Switch(config-if)# hybrid vlan 1000 untagged
Switch(config-if)# pvid 1000
```

Verify the settings by entering the **show vlan** command.

qos aggregate-policer

To define a named aggregate policer for use in policy maps, use the qos aggregate-policer command in global configuration mode. To delete a named aggregate policer, use the no form of this command. The qos aggregate-policer command is for single rate policing and the qos aggregate-policer cir command is for two rate policing.

qos aggregate-policer *NAME BPS [BURST-NORMAL] [BURST-MAX]* **exceed-action** *ACTION* **[violate-action** *ACTION***]**

qos aggregate-policer *NAME* **cir** *CIR* **[bc** *CONFORM-BURST***] pir** *PIR* **[be** *PEAK-BURST***] [exceed-action** *ACTION* **[violate-action** *ACTION***]]**

no qos aggregate-policer *NAME*

Syntax Description	
NAME	Specifies the name of the aggregate policing rule. The NAME parameter can be up to 32 characters, is case sensitive, and may include a-z, A-Z, 0-9, the dash character (-), the underscore character (_), and the period character (.).The policer names must start with an alphabetic character (not a digit) and must be unique across all aggregate policers.
BPS	Average rate, in bits per second. min: 64KB max:32GB
BURST-NORMAL	(Optional) Normal burst size in bytes. Valid values are project dependent. min:4KB max:16MB default:4KB. Unit is KB
BURST-MAX	(Optional) Maximum burst size, in bytes. Valid values are project dependent. min:4KB max:16MB default:4KB. Unit is KB
CIR	Specifies the committed information rate in Kbps. The committed packet rate is the first token bucket for the two-rate metering. min: 64KB max:32GB
PIR	Specifies the peak information rate in Kbps. The peak information rate is the second token bucket for the two-rate metering. min: 64KB max:32GB
CONFORM-BURST	Specifies the burst size for the first token bucket in bytes. min:4KB max:16MB default:4KB.

Syntax Description	
PEAK-BURST	PEAK-BURST Specifies the burst size for the second token bucket in bytes. min: 4KB max: 16MB default :4KB.
exceed-action	Specifies action to take on packets that exceed the rate limit.
violation-action	(Optional) Specifies action to take on packets that violate the normal and maximum burst sizes for singe rate policing. . Specifies the action to take for those packets that did not conform to both CIR and PIR. For two rates policing. If violate-action is not specified for single rate policer, it will create a single rate two color policer.
ACTION	Action to take on packets. Specifies one of the following keywords: "drop-Drops the packet. "set-dscp-transmit VALUE - Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. "transmit-Transmits the packet. The packet is not altered.

Default Not configured

For a two rate policer, the defaults for unspecified options are as follows:

- **exceed-action: drop**.
- **violate-action** equals **exceed-action**

Command Mode Global configuration

Usage Guideline An aggregate policer can be shared by different policy map classes and on different interfaces. It cannot be shared by different policy map.

For detailed description regarding how to configure the policer, refers to the usage guideline for police and police cir command.

Note: Either one of qos aggregate-policer NAME command and qos aggregate-policer NAME cir command can be activated for the refereed traffic class. The latter command will overwrite the previous qos aggregate-policer NAME setting once the reference aggregator name are the same.

Example

In the following example, an aggregate policer named agg-policer5 with single rate two colors is configured. This named aggregator policer is applied as the service policy for the class1 and class2 traffic class in the policy2 policy map.

```
Switch(config)# qos aggregate-policer agg-policer5 10000 128 exceed-action
drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg-policer5
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police aggregate agg-policer5
Switch(config-pmap-c)# exit
```

Verify the settings by entering the **show qos aggregate-policer** command.

qos bandwidth

To set the received bandwidth limit values for an interface, use the bandwidth ingress command in interface configuration mode. To set the transmit bandwidth limit values on an interface use the bandwidth egress command in interface configuration mode. To disable bandwidth limit, use the no form of this command.

qos bandwidth {egress | ingress} *NUMBER-KBPS*

no qos bandwidth {egress | ingress}

Syntax Description	
NUMBER-KBPS	Specifies the number of kilo bytes per second as the limitation on the bandwidth. min: 0KB to max:10MB per second

Default Disabled

Command Mode Interface configuration

Usage Guideline Only physical ports are valid for this command.

The specified limitation should not exceed the maximum speed of the specified interface.

For ingress bandwidth limitation, the ingress will send pause frame or flow control frame when the received traffic exceeds the limitation.

Example In the following example, bandwidth limitations are configured on eth 2.5. The ingress bandwidth is limited to 128 Kbps and the egress bandwidth is limited to 256 Kbps.

```
Switch(config)#interface eth2.5
Switch(config-if)#qos bandwidth ingress 128
Switch(config-if)#qos bandwidth egress 256
```

Verify the settings by entering the **show qos interface bandwidth** command.

qos cos

To configure the default class of service (CoS) value of a port, use the qos cos command in interface configuration mode.

qos cos *COS-VALUE*

Syntax Description	
COS-VALUE	Assigns a default CoS value to a port. This CoS will be with the incoming CoS of the untagged packet received by the port.

Default *COS-VALUE*: 0

Command Mode Interface configuration

Usage Guideline Only physical ports are valid.

Example In the following example, default COS of eth3.1 is set to 3.

```
Switch(config)# interface  eth3.1
switch(config-if)# qos cos 3
```

Verify the settings by entering the **show qos interface cos** command.

qos deficit-round-robin

Use the qos command in interface configuration mode to enable the Deficit Round Robin (DRR)/Weighted Round Robin (WRR) packet scheduling mechanism. To restore the packet scheduling mechanism, use the default form of this command.

qos {deficit-round-robin [*COS-QUEUE* **quantum** *WEIGHT***] |weight-round-robin [***COS-QUEUE* **weight** *WEIGHT***]}**

default qos

Syntax Description	
deficit-round-robin	deficit-round-robin in interface configuration mode to enable the Deficit Round Robin (DRR) packet scheduling mechanism
weight-round-robin	weight-round-robin in interface configuration mode to enable the weighted Round Robin (WRR) packet scheduling mechanism
COS-QUEUE	The transmit priority queue; valid value is from 0 to 7.
quantum *WEIGHT*	(Optional) Specifies the Deficit Round Robin (DRR) quantum weight from 0 to 255. The final quantum is 16Kbytes * WEIGHT. The number of zero stands for strict priority mode.
weight WEIGHT	(Optional) Specifies the WRR weight. The final weight is number of permitted scheduling packets.Tthe range is 0 ~ 15 and the number of zero stands for strict priority mode.

Default

Strict priority mode and DRR mode is disabled.

quantum *WEIGHT*: 1

wrr-*WEIGHT***:** 1

Command Mode

Interface configuration

Usage Guideline

Only physical port interfaces are valid for this command.

The port CoS queue can be either strict priority mode, deficit round robin (DRR)mode or Weight round robin (WRR) mode. The strict priority scheduler mode provides strict priority access to the egress port across the transmit priority queue from the highest priority index to the lowest. The purpose of the strict priority scheduler is to provide lower latency service to the higher CoS classes of traffic.

DRR operates by serving a mount of backlogged credits into the transmit queue in round robin order. Initially, each queue sets its credit counter to a configurable quantum value. Every time a packet from a CoS queue is sent, the size of the packet is subtracted from the corresponding credit counter. When the credit counter drops below 0, the queue is no longer serviced until its credits are replenished.

All queues are serviced until their credit counter is zero or negative and a packet is transmitted completely. As this condition happens, the credits are replenished. When the credits are replenished, as a quantum of credits are added to each CoS queue credit counter. The quantum for each CoS queue may different based on the user configuration.

To set a CoS in strict priority mode, any higher priority CoS must be in strict priority mode. For example, to set CoS 5 in strict priority mode, CoS 6 and 7 have to be in strict priority mode.

WRR operates by transmitting permitted packets into the transmit queue in round robin order. Initially, each queue sets its weight to a configurable weighting. Every time a packet from a higher priority CoS queue is sent, the number of the packet is subtracted from the corresponding weight. When the credit counter reaches zero, the queue is no longer serviced until its weight is replenished. After this repeats for each queue, the next lower priority CoS queue is serviced in turn.

All queues are serviced until their weight is zero and a packet is transmitted completely. As this condition happens, the weights are replenished. When the weights are replenished, weight is added to each CoS queue credit counter. The weight for each CoS queue may different based on the user configuration.

Examples

In the following example, deficit round robin is configured on eth 3.1. For this case, quantum for queue 0 is set to 32 Kbytes; quantum for queue 1 is set to 32 Kbytes; quantum for queue 2 is set to 64 Kbytes; quantum for queue 3 is set to 64 Kbytes; quantum for queue 4 is set to 128 Kbytes; quantum for queue 5 is set to 128 Kbytes; quantum for queue 6 is set to 32 Kbytes; and quantum for queue 7 remains as 0.

```
Switch(config)# interface eth3.1
Switch(config-if)# qos deficit-round-robin 0 quantum 2
Switch(config-if)# qos deficit-round-robin 1 quantum 2
Switch(config-if)# qos deficit-round-robin 2 quantum 4
Switch(config-if)# qos deficit-round-robin 3 quantum 4
Switch(config-if)# qos deficit-round-robin 4 quantum 8
Switch(config-if)# qos deficit-round-robin 5 quantum 8
Switch(config-if)# qos deficit-round-robin 6 quantum 2
Switch(config-if)# qos deficit-round-robin 7 quantum 0
```

In the following example, Weight round robin is configured on eth 3.1. For this case, queue 5, 6, and 7 are set to strict priority mode; weight for queue 4 is set to 4 packets; weight for queue 2, 1, and 0 are set to 2 packets.

```
Switch(config)# interface eth3.1
Switch(config-if)# qos weight-round-robin 0 weight 2
Switch(config-if)# qos weight-round-robin 2 weight 2
Switch(config-if)# qos weight-round-robin 3 weight 2
Switch(config-if)# qos weight-round-robin 4 weight 4
Switch(config-if)# qos weight-round-robin 5 weight 0
Switch(config-if)# qos weight-round-robin 6 weight 0
Switch(config-if)# qos weight-round-robin 7 weight 0
Switch(config-if)# qos weight-round-robin 1 weight 2
Switch(config)#
```

Verify the settings by entering the **show qos interface** command.

qos dscp-mutation

To attach an ingress differentiated-services-code-point (DSCP) mutation map to the interface, use the qos dscp-mutation command in interface configuration mode. To remove the ingress DSCP mutation map from the interface, use the no form of this command.

qos dscp-mutation *DSCP-MUTATION-TABLE-NAME*

no qos dscp-mutation *DSCP-MUTATION-TABLE-NAME*

Syntax Description	
DSCP-MUTATION-TABLE-NAME	Name of the DSCP mutation table. The string of the name is up to 32 characters and no spaces are allowed.

Default Not configured

Command Mode Interface configuration

Usage Guideline Only Physical port interfaces are supported, portchannel interface and vlan interface are not valid for this command.

Use this command to attach an ingress DSCP mutation table to a physical port interface. Use the **"qos map dscp-mutation" on page 499** to configure an ingress DSCP mutation table.

The ingress DSCP mutation will mutate the DSCP value right after the packet is received by the physical port interface.

Example This example shows how to map DSCP 30 to mutated DSCP value 8 and then attach the ingress-DSCP mutation map named mutemap1 to eth 3.1:

```
Switch(config)#qos map dscp-mutation mutemap1 30 to 8
Switch(config)#interface eth 3.1
Switch(config-if)#qos dscp-mutation mutemap1
Switch(config-if)#end
```

Verify the settings by entering the **show qos interface** command.

qos map cos-color

To define the CoS to color map for mapping of a packet's initial color, use the qos map cos-color command in interface configuration mode. To return the map to default setting, use the no form of this command.

qos map cos-color *COS-LIST* **to { green | yellow | red}**

no qos map cos-color

Syntax Description	
COS-LIST	Specifies the list of COS value to be mapped to a color. The range of COS is 0 to 7. The multiple CoS values in the list can be in the form 1, 2,..etc.. separated by commas, a continuous list such as 2-7, or a mixed form 1, 2, 3-5, etc..

Default *COS-LIST:* 0-7 set to green

Command Mode Interface configuration

Usage Guideline Only Physical port interfaces are supported; portchannel interface and vlan interface are not valid for this command.

When a packet entering the ingress port, it will be colored based on either the DSCP to color map (as the port is trust DSP) or CoS to color map (as the port is trust CoS).

Use the qos map cos-color command in interface configuration mode to configure the CoS to color map. If the ingress port is trust CoS, the received packet will be initialized to color based on this map.

Example The following example defines CoS 1-7 as red color, 0 as green color at eth 3.1.

```
Switch(config)# interface eth3.1
Swtich (config-if)# qos map cos-color 1-7 to red
```

Verify the settings by entering the **show qos interface map** command

qos map dscp-color

To define the DSCP to color map for mapping of packet's initial color, use the qos map dscp-color command in interface configuration mode. To return the map to the default setting, use the no form of this command.

qos map dscp-color *DSCP-LIST* **to { green | yellow | red}**

no qos map dscp-color

Syntax Description	
dscp *DSCP-LIST*	Specifies the list of DSCP code point to be mapped to a color. The range of DSCP is 0 to 63. The multiple DSCP values in the list can be in the form 1, 2, etc. separated by commas, a continuous list such as 2-7, or a mixed form 1, 2, 3-10, 63,etc.

Default *DSCP-LIST:* 0-63 mapped to green

Command Mode Interface configuration

Usage Guideline Only physical ports are valid for this command.

When a packet enters the ingress port, it will be colored based on either the DSCP to color map (as the port is trust DSP) or CoS to color map (as the port is trust CoS).

Use the qos map dscp-color command in interface configuration mode to configure the DSCP to color map. If the ingress port is set to trust DSCP, the received IP packet will be initialized to a color based on this map. The non-IP packet will be initialized to a color based on the CoS to color map.

Example The following example defines DSCP61~63 as yellow color, others are green color at eth 3.1.

```
Switch(config)# interface eth3.1
Swtich (config-if)# qos map dscp-color 61-63 to yellow
```

Verify the settings by entering the **show qos interface map** command.

qos map dscp-cos

To define a differentiated services code point (DSCP)-to-class of service (CoS) map, use the qos map dscp-cos command in global configuration mode. To remove a prior entry, use the no form of this command.

qos map dscp-cos *DSCP-LIST* **to** *COS-VALUE*

no qos map dscp-cos

Syntax Description	
dscp-cos *DSCP-LIST* **to** *COST-VALUE*	Specifies the list of DSCP code point to be mapped to a COS value. The range of DSCP is 0 to 63. The series of DSCPs can be separated by comma (,) or hyphen(-). No space is before and after , or -. The COS-VALUE range is 0 ~ 7

Default

Below is a table of the default dscp-cos mappings:

DSCP	ValueCOS Value
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Command Mode

Interface Configuration

Usage Guideline

The DSCP to CoS map is used by the DSCP trust port to map the DSCP value to an internal CoS value, which will be in turn be mapped to the CoS queue based on the CoS to queue map configured by the qos map cos command.

Only physical ports are valid for this command. All of the DSCP-to-CoS maps are globally defined. The map applies to all ports.

Example

This example configures the DSCP to CoS map for mapping DSCP 12, 16, 18 to CoS 1 for eth2.6.

```
Switch(config)# interface eth2.6
Switch(config-if)# qos map dscp-cos 12,16,18 to 1
Switch(config-if)#end
```

Use the **show qos interface map** privileged EXEC command to verify the settings.

qos map dscp-mutation

To define a named differentiated services code point (DSCP) mutation map, use the qos map dscp-mutation command in global configuration mode. To return to the default mapping, use the no form of this command.

qos map dscp-mutation *MAP-NAME INPUT-DSCP-LIST* **to** *OUTPUT-DSCP*

no qos map dscp-mutation *MAP-NAME*

Syntax Description	
MAP-NAME	Name of the DSCP mutation map in a string length up to 32 characters (no space is allowed)
INPUT-DSCP-LIST	Specifies the list of DSCP code point to be mutated to another DSCP value . The range of DSCP is 0 to 63. A series of DSCPs can be separated by comma (,) or hyphen(-). No space is before and after , or -.
OUTPUT-DSCP	Mutated DSCP value; valid values are from 0 to 63.

Default *OUTPUT-DSCP* equals the *INPUT-DSCP*

Command Mode Global configuration

Usage Guideline When a packet is received by an interface, the incoming DSCP can be mutated to another DSCP right before any QoS operations based on the DSCP mutation map.

The DSCP mutation is helpful to integrate domains with different DSCP assignment.

When configuring a named DSCP mutation map, note the following:

- Multiple commands can be entered to map additional DSCP values to a mutated DSCP value.
- A separate command can be entered for each mutated DSCP value.

Up to 15 ingress-DSCP mutation maps can be configured to mutate the incoming DSCP value before any QoS operation. After the ingress-DSCP mutation map creation, use **qos dscp-mutation** command to attach the ingress-DSCP mutation map to physical interfaces.

The DSCP-CoS map and DSCP-color map will still base on packet's original DSCP. All the subsequent operations will base on mutated DSCP.

Example This example shows how to map DSCP 30 to mutated DSCP value 8, DSCP 20 to mutated DSCP 10, the mutation map named, mutemap1:

```
Switch(config)#qos map dscp-mutation mutemap1 30 to 8
Switch(config)#qos map dscp-mutation mutemap1 20 to 10
```

Use the **show qos map** privileged EXEC command to verify the settings.

qos trust

To set the trust state of a port, use the qos trust command in interface configuration mode; to trust either the CoS field or the DSCP field of the arriving packet for subsequent QoS operation.

qos trust { cos | dscp }

Syntax Description	
cos	Specifies that the CoS bits of the arriving packets are trusted for subsequent QoS operations.
dscp	Specifies that the ToS/DSCP bits, if available in the arriving packets, are trusted for subsequent operation. For non-IP packet, L2 CoS information will be trusted for traffic classification.

Default DSCP is trusted.

Command Mode Interface configuration

Usage Guideline Only physical ports are valid for this command. When the interface is set to trust DSCP, the DSCP of the arriving packet will be trusted for the subsequent QoS operations. First the DSCP will be mapped to an internal CoS value, which will in turn determine the CoS queue. The DSCP to COS map is configured by the qos map dscp-cos command. The CoS to queue map is configured by the qos map cos command. If the arriving packet is a non-IP packet, the CoS is trusted.

When the interface is in trust CoS state, the CoS of the coming packet will be the internal CoS and determine the CoS queue based on the CoS to queue map.

When a packet is received by the ingress port, it will be initialized to a color based on the qos map dscp-color if the receipt port is trust DSCP or qos map cos-color if the receipt port is set to trust CoS.

Example This example shows how to set eth3.1 to trust DSCP mode.

```
Switch(config)# interface eth3.1
Switch(config-if)# qos trust dscp
Switch(config-if)# end
```

Verify the settings by entering the **show qos interface** command.

reboot

Use this command to reboot a module on the specified slot. The module can be either a control module or a line card control module.

reboot [unit *UNIT-ID* **]**

Syntax Description	
UNIT-ID	Specifies the unit id.

Default None

Command Mode. Privileged EXEC level 15

Usage Guideline This command is only available for privilege level 15 and above.

This command can be used to reboot a module in a specific slot. If no unit ID is specified, all of the modules in the system will be rebooted.

If the CM module is specified to be reboot, then the entire system (all modules) will reboot.

Note:

Example The following example reboots the whole system:

```
DGS-6600:15#reboot

Warning: This command will cause system reboot.
Do you want to continue (y/n) [n]?y
Save log message before reboot(y/n) [n]?y
```

redistribute

Use redistribute to redistribute routes from one routing domain into BGP. Use no command to disable route redistribution.

redistribute PROTOCOL **[route-map** MAP-NAME**]**

no redistribute PROTOCOL

Syntax Description	
PROTOCOL	Specifies the protocol whose routes are to be redistributed. It can be one of the following keywords **connected, ospf, rip static.** The **static** keyword means to redistribute IP **static** routes. The **connected** keyword refers to routes that are established automatically by virtue of having enabled IP on an interface.
route-map *MAP-NAME*	(Optional) Specify the identifier of a route map used to filter the networks to be redistributed. If not specified, all networks are advertised.

Default Route redistribution is disabled.

Command Mode. Router configuration

Address family configuration

Usage Guideline **Note:** The user can use the command to redistribute prefix from different sources to BGP protocol.

Example The following example redistributes the OSPF process routes into BGP process.

```
Switch(config)# router bgp 8001
Switch(config-router)# redistribute ospf
Switch(config-router)# end
Switch#
```

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

redistribute (OSPF)

Use **redistribute** to redistribute routes from other routing domain into OSPF routing domain. Use the no form of the command to disable redistribution.

redistribute *PROTOCOL* **[metric** *METRIC-VALUE***] [metric-type** *TYPE-VALUE***]**

no redistribute *PROTOCOL*

Syntax Description	
PROTOCOL	The source protocol from which routes are being redistributed from. It can be one of thefollowing keywords: bgp, connected, static, or rip. The static keyword is used to redistribute IP static routes. The connected keyword refers to routes that are established automatically by virtue of having enabled IP on an interface. For routing protocols such as Open Shortest Path First (OSPF), these routes will be redistributed as external to the autonomous system.
metric *METRIC-VALUE*	(Optional) If a metric is not specified, OSPF puts a default value of 20 as redistributing routes from all other protocols except Border GatewayProtocol (BGP) routes, which get a metric of 1. However when redistributing from one OSPF process to another OSPF process, the metric will be carried through.
metric-type *TYPE-VALUE*	(Optional) For OSPF, the external link type associated with the route advertised into the OSPF routing domain. It can be one of two values: 1-Type 1 external route 2-Type 2 external route. If a metric-type is not specified, the Switch adopts a Type 2 external route. This is only for OSPF.

Default Disabled

metric-type *TYPE-VALUE:* Type 2 external route

Command Mode Router configuration

Usage Guideline A router receiving a link-state protocol with 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.

Whenever the **redistribute** or the **default-information originate** configuration commands are used to redistribute routes into an OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a default route into the OSPF routing domain.

BGP, RIP, connected, static routes can be redistributed to OSPF.

The redistribute metric is determined by following rules in order:

1. If the redistribute metric is specified, use the user specified value.

2. If the redistribute route is default route, the metric will be 1.

3. If "default metric" is configured, use the specified value.

4. If the "default metric" is not configured, and the route is redistributed from BGP. The metric will be 1.

5. If the "default metric" is not configured, and the route is not redistributed from BGP. the metric will be 20.

BGP, RIP can be redistributed to OSPF.

If a metric is not specified, OSPF puts a default value of 20 and redistributes routes from all other protocols except Border Gateway.

Example This example shows how to BGP routes are redistributed into a OSPF domain:

```
Switch(config)# router ospf
Switch(config-router)# redistribute bgp 100
Switch(config-router)#end
Switch#
```

Verify the settings by entering the **show ip protocols ospf** command.

redistribute (IPv6 OSPF)

Use redistribute to redistribute routes from other routing domains into the IPv6 OSPF routing domain. Use the no form of the command to disable redistribution.

redistribute *PROTOCOL* **[metric** *METRIC-VALUE*] **[metric-type** *TYPE-VALUE*]

no redistribute *PROTOCOL*

Syntax Description	
*PROTOCO*L	Source protocol from which routes are being redistributed. It can be one of the following keywords: connected, static, or rip.
METRIC-VALUE	(Optional) When redistributing from one OSPF process to another OSPF process on the same router, the metric will be carried through from one process to the other if no metric value is specified.
TYPE-VALUE	(Optional) IPv6 OSPF specifies the external link type associated with the default route advertised into the IPv6 OSPF routing domain. It can be one of two values: 1: Type 1 external route 2: Type 2 external route If a metric-type is not specified, the Switch adopts a Type 2 external route. This is only for IPv6 OSPF.

Default Disabled

Command Mode Router configuration

Usage Guideline Changing or disabling any keyword will not affect the state of other keywords.

A router receiving a link-state protocol with 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.

Whenever the **redistribute** or the **default-information originate** configuration commands are used to redistribute routes into an IPv6 OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a default route into the IPv6 OSPF routing domain.

When routes are redistributed into IPv6 OSPF from protocols other than IPv6 OSPF, and no metric has been specified with the metric-type keyword and type-value argument, IPv6 OSPF will use 20 as the default metric. When intra-area and inter-area routes are redistributed between IPv6 OSPF processes, the internal OSPF metric from the redistribution source process is advertised as the external metric in the redistribution destination process.

Routes configured with the connected keyword affected by this redistribute command are the routes not specified by the router configuration command.

The **default-metric** command cannot be used to affect the metric used to advertise connected routes.

Example

In the example, IPv6 OSPF redistributes any prefixes that have been learned through IPv6.

```
Switch> enable
Switch# configure terminal
Switch(config)# router ipv6 ospf
Switch(config-router)# redistribute rip metric 10
```

redistribute (RIP)

Use redistribute to redistribute routes from one routing domain into another routing domain. Use the no form of the command to disable redistribution.

redistribute *PROTOCOL* **[metric** *METRIC-VALUE***]**

no redistribute *PROTOCOL*

Syntax Description	
PROTOCOL	Source protocol from which routes are being redistributed. It can be one of the following keywords: bgp, connected, ospf, static. The static keyword is used to redistribute IP static routes. The connected keyword refers to routes that are established automatically by virtue of having enabled IP on an interface. For routing protocols such as Open Shortest Path First (OSPF), these routes will be redistributed as external to the autonomous system.
metric *METRIC-VALUE*	(Optional) Specifies metric value to be used in redistributing information. The range is 0 to 16. Regarding the metric conversion, the following is the rule. 1. If the metric is not specified, the metric for the redistributed route from other protocols to the RIP process will be determined by the value of the "default-metric" command. 2. If the metric is specified as 0, the metric for the redistributed route from other protocols to the RIP process will be 1.

Default Disabled

PROTOCOL: Not configured

METRIC-VALUE: 0

Command Mode Router configuration

Usage Guideline Routes, configured with the connected keyword, affected by this redistribute command are the routes not specified by the network router configuration command.

Regarding the metric conversion, the following is the rule.

If the metric option is not specified, the following rules are applied:

1. If the metric is not specified, or is specified as 0, the metric for the redistributed static route or connected route will be 1.
2. If the metric is not specified, the metric for the redistributed route from other protocols to RIP process will be determined by the value of the “**default-metric**” command.

3. If the metric is specified as 0, the metric for the redistributed route from other protocols to RIP will be 1.

If the **default-metric** is not specified, then the original metric from the redistributed protocol will be transparently carried through.

1. The **default-metric** command cannot be used to affect the metric used to advertise connected routes.
2. The metric value specified in the **redistributed** command supersedes the metric value specified using the **default-metric** command.

Examples

This example shows OSPF routes are redistributed into a RIP domain:

```
Switch(config)# router rip
Switch(config-router)# redistribute ospf
Switch(config-router)# end
Switch#
```

The following example causes the specified OSPF routes to be redistributed into an RIP domain. The OSPF-derived metric will be remapped to 11.

```
Switch(config)# router rip
Switch(config-router)# redistribute ospf metric 11
Switch(config-router)# end
Switch#
```

Verify the settings by entering the **show ip protocols rip** command.

redistribute (RIP IPv6)

Use redistribute to redistribute routes from one routing domain into another routing domain. Use no command to disable redistribution.

redistribute *PROTOCOL* **[metric** *METRIC-VALUE***]**

no redistribute *PROTOCOL*

Syntax Description	
PROTOCOL	Source protocol from which routes are being redistributed. It can be one of the following keywords: connected, ospf, and static.
METRIC-VALUE	(Optional) Specifies metric value to be used in redistributing information. The range is 0 to 16.

Default

Disabled

PROTOCOL: Not configured

METRIC-VALUE: 1.

Command Mode

Router configuration

Usage Guideline

Routes configured with the connected keyword affected by this redistribute command are the routes not specified by the network router configuration command.

Regarding the metric conversion, the following is the rule.

If the metric option is not specified, the following rules are applied:

1. If the metric is not specified, or is specified as 0, the metric for the redistributed static route or connected route will be 1.
2. If the metric is not specified, the metric for the redistributed route from other protocols to RIP process will be determined by the value of the "default-metric" command.

3. If the metric is specified as 0, the metric for the redistributed route from other protocols to RIP process will be 1.

Also, if the default-metric is not specified, then the original metric from the redistributed protocol will be transparently carried through.

1. The **default-metric** command cannot be used to affect the metric used to advertise connected routes.
2. The metric value specified in the redistribute command supersedes the metric value specified using the default-metric command.

Example The following example causes the specified OSPF process routes to be redistributed into an RIPng domain. The metric will be remapped to 10.

```
Switch > enable
Switch # configure terminal
Switch (config) # router ipv6 rip
Switch (config-router) # redistribute ospf metric 10
```

remote-span

Use the command to specify a VLAN as a RSPAN VLAN. Use the no form of the command to revert to a non RSPAN VLAN.

remote-span

no remote-span

Syntax Not applicable

Default 802.1q VLAN

Command Mode VLAN config mode

Usage Guideline Use the remote-span command in vlan config mode to specify a VLAN as a RSPAN VLAN. When a VLAN is specified as a RSPAN VLAN, the access member port of the VLAN will become inactive. The MAC address learning on the RSPAN VLAN is disabled.

Use the command in the source switch, middle switch and the destination switch involved in the RSPAN session.

For the middle switch involved in a RSPAN session, the port that the monitored packet arrives from and the port that the monitored packets will be sent out need to configured as tag member port of the RSPAN VLAN.

Example This example assigns VLAN 100 as the RSPAN VLAN in the middle switch of RSPAN session. Supposed that eth3.1 is where the monitored packets arrive and eth3.5 is where the monitored packet is transmitted.

```
Switch(config)# interface eth3.1
Switch(config-vlan)# trunk allowed-vlan 100
Switch(config-vlan)# exit
Switch(config)# interface eth3.5
Switch(config-vlan)# trunk allowed-vlan 100
Switch(config-vlan)# exit
Switch(config)# vlan 100
Switch(config-vlan)# remote-span
Switch(config-vlan)#exit
Switch(config)#
```

You can verify your settings by entering the show vlan command.

resequence access-list

Use this command to re-sequence the priority of the access-list entries in an access-list (mac, ip or ipv6 access list).

resequence access-list *NAME STARTING-SEQUENCE-NUMBER INCREMENT*

Syntax Description	
NAME	The name of the MAC, IP or IPv6 access-list to be configured. It can accept up to 32 characters. The syntax is a general string that does not allow space.
STARTING-SEQUENCE-NUMBER	Access list entries will be resequenced using this initial value. The default value is 10. The range of possible sequence numbers is 1 through 65535.
INCREMENT	The number by which the sequence numbers change. The default value is 10. For example, if the increment value is 5 and the beginning sequence number is 20, the subsequent sequence numbers are 25, 30, 25, 40, and so on. The range of *INCREMENT* is 1 through 65535.

Default Disabled

Command Mode Global configuration

Usage Guideline This feature allows the **permit** and **deny** entries of a specified access list to be re-sequenced with an initial priority value determined by the *STARTING-SEQUENCE-NUMBER* argument, and continuing in increments determined by the *INCREMENT* argument. If the highest priority exceeds the maximum possible sequence number, then no sequencing occurs.

If entries with no priority are applied, the first entry is assigned a priority of 10, and successive entries are incremented by 10.

If the user enters an entry without a priority, it is assigned a priority that is 10 greater than the largest priority value (with least priority) in that access list and is placed at the end of the list.

Example This example shows how to re-sequence the priority of IP access-list, named *R&D*

```
Switch(config)# show access-list ip R&D
10 permit tcp any 10.20.0.0 255.255.0.0
20 permit tcp any host 10.100.1.2
30 permit icmp any any
Switch(config)# resequence access-list R&D 1 2
Switch(config)# show access-list ip R&D
1 permit tcp any 10.20.0.0 255.255.0.0
3 permit tcp any host 10.100.1.2
5 permit icmp any any
```

revision

To set the revision number for the MST configuration, use the revision command. To return to the default settings, use the no form of this command.

revision *REVISION*

no revision

Syntax Description	
REVISION	When a switch using the same given name but with a different revision level than another switch, then the two switches are considered members of different MST regions. The range is 0 to 65535.

Default *REVISION*: 0

Command Mode MST configuration

Usage Guideline If Two DGS-6604 series Ethernet switches have the same configuration but with different revision numbers, then they are considered to be part of two different regions.

Caution: Be careful when using the revision command to set the revision number of the MST configuration because a mistake can put the switch in a different region.

Example This example shows how to configure the revision level of MSTP configuration to 2.

```
Swtich(config)# spanning-tree mst configuration
Switch(config-mst)#revision 2
```

Verify the settings by entering the **show spanning-tree mst configuration** command.

rmon statistics

Use the rmon collection stats interface configuration command to collect Ethernet group statistics, Use the no form of this command to return to disable RMON entry.

rmon statistics *ENTRY-NUMBER* **[owner** *NAME***]**

no rmon statistics *ENTRY-NUMBER*

Syntax Description	
ENTRY-NUMBER	Remote Network Monitoring (RMON) table index. The range is 1 to 65535.
owner *NAME*	(Optional) Name of the owner that configured this entry and is using its assigned resources. The length of the name can be from 1 to 255 characters.

Default Disabled

Command Mode Interface configuration

Usage Guideline This command allows the administrator to enable or disable RMON on Ethernet interfaces of the device. If the administrator enables the RMON mechanism on the specific interface, the device will automatically collect statistical information about the traffic for the interface. The administrator can also perform operations on the supported MIB RMON groups.

Examples This example shows how to create two RMON entries on Ethernet interface 3.2.

```
Switch# configure terminal
Switch(config)#interface eth3.2
Switch(config-if)#rmon statistics 3 owner monitor
Switch(config-if)#rmon statistics 4
```

This example shows how to disable the RMON entry on Ethernet interface 3.2.

```
Switch#configure terminal
Switch(config)#interface eth3.2
Switch(config-if)#no rmon statistics 3
```

route-map

Use route-map to add the policy routing entry. Use the no form of the command to remove a policy routing entry.

route-map *MAP-NAME* **{ permit | deny }** *SEQUENCE-NUM*

no route-map *MAP-NAME* **[permit** *SEQUENCE-NUM* **| deny** *SEQUENCE-NUM* **]**

Syntax Description	
MAP-NAME	A meaningful name for the route map. Multiple route maps may share the same map tag name
permit	(Optional) If the match criteria is met for this route map, and the permit keyword is specified, the route is redistributed as controlled by the set actions. In the case of policy routing, the packet is policy routed. If the match criteria is not met, and the permit keyword is specified, then the next route map with the same map tag will be tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it will not be redistributed by that set.
deny	(Optional) If the match criteria is met for the route map and the deny keyword is specified, then the route will not be redistributed. In the case of policy routing, the packet will not be policy routed, and no further route maps sharing the same map tag name will be examined. If the packet is not policy routed, then the normal forwarding algorithm will be used.
SEQUENCE-NUM	(Optional) A number that indicates the position a new route map will have in the list of route maps already configured with the same name. When used with the no form of this command, the position of the route map will be deleted.

Default **permit**

Command Mode Global configuration

Usage Guideline Use the route-map command to enter route-map configuration mode.

The route map can be used in route redistribution, route filtering, and policy route application.

A route map could be defined by multiple route map statements. These route map statements share the same map name. The statement with a lower sequence number has higher priority. Within the same route map, multiple match statements and multiple set statements can be defined. To meet a specific route map statement, all of the match statements must be met. When a route map statement is met, all of the set statements defined in this route map statement will be performed. Subsequent route map statements for the same route map will not be searched.

If the no route-map MAP-TAG command is specified (with no SEQUENCE-NUM argument), the entire route map is deleted.

Example This example shows how to add the policy routing entry with name "myPolicy":

```
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)#match community Mycommunity
Switch(config-route-map)#set weight 1000
Switch(config-route-map)#end
Switch#
```

Verify the settings by entering the **show running-config** command.

router bgp

Use this command to enable (configure) BGP routing process. Use the no form of the 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. The range for 2-byte numbers is 1 to 65535. The range for 4-byte numbers is 65536 to 4294967295 or 1.0 to 65535.65535.

Default Disabled

Command Mode Global configuration

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.

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.

Example This example shows how to configure a BGP process for autonomous system 1.65534:

```
Switch(config)# router bgp 1.65534
Switch(config-router)#
```

router-id

Use this command to specify a router ID for the OSPF process. Use the no form of the command to revert to the automatic determination of router-id.

router-id *IP-ADDRESS*

no router-id

Syntax Description	
IP-ADDRESS	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.

Command Mode Router configuration

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. Each router must be configured with a unique router-id.

If this command is used on an active OSPF router process (already has neighbors), the new router-ID will not take effect immediately. It will be used at the next reload or at a manual OSPF process restart.

Example This example shows how to configure router id to 10.10.10.60

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# router-id 10.10.10.60
```

Verify the settings by entering the **show ip protocols ospf** command.

router-id (IPv6)

To assign a fixed router ID, use the router-id command in router configuration mode, and force IPv6 OSPF routing process with the previous IPv6 OSPF router ID. To disable this function, use the no form of this command.

router-id *IP-ADDRESS*

no router-id

Syntax Description	
IP-ADDRESS	Router ID in IPv4 address format.

Default The router-id is automatically chosen based on the highest IP address present on the router.

Command Mode Router configuration

Usage Guideline Router ID is a 32-bit number assigned to each router running the IPv6 OSPF protocol. This number uniquely identifies the router within an Autonomous System. Each router must be configured with a unique router-id.

If this command is used on an active IPv6 OSPF router process (already has neighbors), the new router ID will not take effect immediately. It is used at the next reload or at a manual restart of IPv6 OSPF process.

Example The following example specifies a fixed router ID.

```
Switch > enable
Switch # configure terminal
Switch (config) # router ipv6 ospf
Switch (config-router) # router-id 10.1.1.1
```

router ipv6 rip

To configure an IPv6 RIP routing process, use the router ipv6 rip command in global configuration mode. To remove a routing process, use the no form of this command.

router ipv6 rip

no router ipv6 rip

Syntax None

Default Not configured

Command Mode Global configuration

Usage Guideline The router ipv6 rip command is similar to the router rip command, except that it is IPv6-specific. Use this command to enable an IPv6 RIP routing process globally. Using this command places the router in router configuration mode for the IPv6 RIP routing process. The router prompt changes to Switch(config-router)#.

Example The following example configures the IPv6 RIP routing process and places the router into router configuration mode for the IPv6 RIP routing process.

```
Switch > enable
Switch # configure terminal
Switch (config) # router ipv6 rip
Switch(config-router)# end
```

router ipv6 ospf

To enable the IPv6 OSPF routing process, use the router ipv6 ospf command in global configuration mode. To disable this function, use the no form of this command.

router ipv6 ospf *[PROCESS-ID*]

no router ipv6 ospf [*PROCESS-ID***]**

Syntax Description	
PROCESS-ID	(Optional) Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.

Default Not configured

PROCESS-ID: null

Command Mode Global configuration

Usage Guideline Use this command to enter the router configuration mode of IPv6 OSPF. In this mode, there are other setting of IPv6 OSPF that can be configured.

Example The following example enables router OSPF for IPv6 configuration mode.

```
Switch > enable
Switch # configure terminal
Switch (config) # router ipv6 ospf 0
Switch (config-router) #
```

router ospf

To configure an Open Shortest Path First (OSPF) routing process, use the router ospf command in global configuration mode. To terminate an OSPF routing process, use the no form of this command.

router ospf

no router ospf

Syntax None

Default Not configured

Command Mode Global configuration

Usage Guideline This command is used to enable OSPF routing processes and enter into router configuration mode then other OSPF-related settings can be configured.

Example This example shows how to enable ospf and enter the ospf router configuration mode.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)#
```

Verify the settings by entering the **show ip protocols ospf** command.

router rip

Use the command to configure the RIP routing process. To turn off the RIP routing process, use the no form of this command.

router rip

no router rip

Syntax None

Default Not configured

Command Mode Global configuration

Usage Guideline This command is used to enable the RIP function and enter the Router configuration mode of RIP protocol.

Executing the no form of the command, will remove the configuration in the router mode.

Example The following example shows how to begin the RIP routing process:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# end
```

Verify the settings by entering the **show ip protocols rip** command.

send-lifetime

To set the time period during which an authentication key on a key chain is valid to be sent, use the send-lifetime command in key chain key configuration mode.

send-lifetime *START-TIME* **{infinite |** *END-TIME* **| duration** *SECONDS***}**

Syntax Description	
START-TIME	The beginning time that the key specified, by the key command, is valid to be received. The syntax can be either of the following: HH:MM:SS MONTH DATE YEAR HH:MM:SS DATE MONTH YEAR HH-hours MM-minutes SS-seconds MONTH-first three letters of the month DATE-date (1-31) YEAR-year (four digits) The default start time and the earliest acceptable date is January 1, 1993.
infinite	Key is valid to be sent from the start-time value on and will not expire.
END-TIME	Key is valid to be sent from the start-time value until the end-time value.The syntax is the same as that for the START-TIME. The end-time value must be after the start-time value. The default end time is an infinite time period.
duration *SECONDS*	Length of time (in seconds) that the key is valid to be sent. The range is from 1 to 2147483647 (signed long).

Default **infinite**

Command Mode Key-chain key configuration

Usage Guideline Specify a start-time value and one of the following values: infinite, end-time, or duration seconds.

if lifetimes are to be configured on keys, then it is recommended to use Network Time Protocol (NTP) or another similar time synchronization method.

When there are multiple keys that are valid at a time, the first valid key will be used. If there are no valid keys during a specific period of time, then no authentication will be performed.

Example

The following example configures a key chain named chain1. Key 1 named "forkey1string" will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. Key3 named "forkey3string" will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m.

```
Switch(config)# interface vlan1
Switch(config-if)# ip rip authentication key-chain chain1
Switch(config-if)# ip rip authentication mode text
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 172.19.0.0/8
Switch(config-router)# version 2
Switch(config-router)# exit
Switch(config)# key chain chain1
Switch(config-keychain)# key 1
Switch(config-keychain-key)# key-string forkey1string
Switch(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2009 duration 7200
Switch(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2009 duration 3600
Switch(config-keychain-key)# exit
Switch(config-keychain)# key 3
Switch(config-keychain-key)# key-string forkey3string
Switch(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2009 duration 7200
Switch(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2009 duration 3600
Switch(config-keychain-key)# exit
Switch(config-keychain)# exit
```

Verify the settings by entering the **show ip key-chain** command.

server

Set up a server for different types of methods. Use the no form of this command to delete a server.

server {tacacs | xtacacs} *IP-ADDRESS* **[auth-port** *PORT-NUMBER***] [timeout** *SECONDS***] [retransmit** *COUNT* **]**

server tacacs+ *IP-ADDRESS* **[auth-port** *PORT-NUMBER***] {key** *KEY-STRING* **| no-encrypt}**

server radius *IP-ADDRESS* **[auth-port** *PORT-NUMBER***] {key** *KEY-STRING* **| no-encrypt} [timeout** *SECONDS* **] [retransmit** *COUNT* **]**

no server {tacacs | xtacacs | tacacs+ | radius} *IP-ADDRESS*

Syntax Description	
tacacs	Specifies tacacs authentication.
xtacacs	Specifies xtacacs authentication.
tacacs+	Specifies tacacs+ authentication.
radius	Specifies radius authentication.
IP-ADDRESS	Specifies the IP address of the authentication sever.
auth-port *PORT-NUMBER*	(Optional) Specifies theTCP or UDP destination port for authentication requests. The port-number argument specifies the port number for authentication requests.
key *KEY-STRING*	The key for TACACS+ or RADIUS authentication. This argument is only present for TACACS+ and RADIUS. The key can be from 1 to 32 characters. The syntax is a general string that does not allow space.
no-encrypt	No encryption for TACACS+ and RADIUS authentication. This argument is only present for TACACS+ and RADIUS.
timeout *SECONDS*	The time in seconds for waiting server reply. The range of timeout is 1 - 255 seconds.
retransmit *COUNT*	Specifies the number of switch system resend an authentication request to the server when no response is received. The value is from 0 to 3, and 0 to disable the retransmit.

Default

radius auth-port *PORT-NUMBER***:** 1812

tacacs/xtacacs/tacacs+ auth-port *PORT-NUMBER*: 49

timeout: 5 seconds

retransmit: 2

Command Mode

aaa group server configuration

Usage Guideline

Enable TACACS, XTACACS, TACACS+, or RADIUS authentication method for login and enable access to the switch. The first created authentication method will be the primary one. The maximum number of entries in the list is project

dependent. However it is recommended to be 3 and use them as a backup server scheme.

The encryption key is used to encrypt and authenticate all communication between the TACACS+/RADIUS client and server. The same key must be configured on the client and the server.

Example

The following example shows the network access server configured to recognize two RADIUS host entries. The second host entry configured acts as fail-over backup to the first one (the RADIUS host entries are tried in the order in which they are configured).

```
Switch(config)#aaa group server group1
Switch(config-aaa-groug-server)# server radius 172.19.10.100 auth-port 1500 key 12345678
Switch(config-aaa-group-server)# server radius 172.19.10.100 auth-port 1600 key 12345678
Switch(config-aaa-group-server)# end
Switch(config)#
```

Verify the settings by entering the **show aaa group server** command.

service dhcp

Use this command to enable a Dynamic Host Configuration Protocol (DHCP) server features on the switch. Use the no form of this command to disable DHCP server features.

service dhcp

no service dhcp

Syntax None

Default Disabled

Command Mode Global configuration

Usage Guideline Use this command to enable DHCP server function. The DHCP server function is disabled by default.

Example Enable DHCP server function:

```
switch > enable
switch# configure terminal
switch(config)# service dhcp
```

service-policy

To attach a policy map to an input interface use the service-policy command in the interface configuration mode. To remove a service policy from an input interface, use the no form of this command.

service-policy *NAME*

no service-policy *NAME*

Syntax Description	
NAME	The name of a service policy map (created using the policy-map command) to be attached. The name can be a maximum of 32 alphanumeric characters.

Default None

Command Mode Interface configuration

Usage Guideline Only physical port interfaces are valid for this command.

Use the **service-policy** command to attach a single policy map to input interfaces. This policy is attached to the interface for aggregate and controls the number or rate of packets. The packet arriving at a port will be treated based on the service policy attached to the interface.

A policy map needs to be created before it is specified in this command.

A policy map without a configured class policy can not be attached.

Examples In the following example shown on the next page, two policy maps are defined-cust1-classes, and cust2-classes.

For cust1-classes, gold is configured to use CoS Queue 6 and policed by a single rate policer with an average rate set to 64 Kbits per second and a normal burst size set to 128 Kbytes. Silver is configured to use CoS queue 5 and policed by a single rate policer with an average rate set to 64 Kbits per second and the normal burst size set to 128 Kbytes. Bronze is configured to use CoS queue 0 and policed by a single rate policer with an average rate set to 64 Kbits per second and a normal burst size set to 128K bytes.

For cust2-classes, gold is configured to use CoS Queue 6 and policed by a single rate policer with an average rate set to 128 Kbits per second and the normal burst size set to 256 Kbytes. Silver is policed by a single rate policer with an average rate set to 128 Kbits per second and the normal burst size set to 256 Kbytes. Bronze is policed by a single rate policer with an average rate set to128 Kbits per second and the normal burst size set to 256 Kbytes.

The cust1-classes policy map is configured and then attached to eth3.1 and eth3.2 by the following commands.

```
Switch(config)# class-map gold
Switch(config-cmap)# match cos 6
Switch(config-cmap)# exit
Switch(config)# class-map silver
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
Switch(config)# class-map bronze
Switch(config-cmap)# match cos 0
Switch(config-cmap)# exit
Switch(config)# policy-map cust1-classes
Swtich(config-pmap)# class gold
Switch(config-pmap-c)# police 64 128 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# police 64 128 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze
Switch(config-pmap-c)# police 64 128 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface eth3.1
Switch(config-if)# service-policy cust1-classes
Switch(config-if)# exit
Switch(config)# interface eth3.2
Switch(config-if)# service-policy cust1-classes
Switch(config-if)# exit
```

The cust2-classes policy map is configured and then attached to eth4.1by the following commands.:

```
Switch(config)# policy-map cust2-classes
Swtich(config-pmap)# class gold
Switch(config-pmap-c)# police 128 256 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# police 128 256 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze
Switch(config-pmap-c)# police 128 256 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface eth4.1
Switch(config-if)# service-policy cust2-classes
Switch(config-if)# exit
```

Verify the settings by entering the **show qos interface** command.

set

Use the set command in policy map class configuration mode to set the new precedence field, DSCP field, and CoS field of the out-going packet. The user can also directly specify the CoS queue for the packet.

set { [ip] precedence *PRECEDENCE* **| [ip] dscp** *DSCP* **| cos** *COS* **| internal-cos** *COS***}**

no set { [ip] precedence *PRECEDENCE* **| [ip] dscp** *DSCP* **| cos** *COS* **| internal-cos** *COS***}**

Syntax Description	
precedence *PRECEDENCE*	Specifies a new precedence for the packet. The range is 0 to 7. If the optional keyword **ip** is specified, then the IPv4 precedence will be marked. Note that setting of precedence will not affect the CoS queue selection.
dscp *DSCP*	Specifies a new DSCP for the packet. The range is 0 to 63. The optional keyword ip is specified, then the IPv4 DSCP will be marked. Note that setting of DSCP will not affect the CoS queue selection.
cos *COS*	Assigns a new cos value to the packet. The range is 0 to 7. Note that setting of CoS will not affect the CoS queue selection.
internal-cos *COS*	Assigns the CoS queue to the packet. This overwrite the original CoS queue selection.

Default Not configured

Command Mode Policy-map class configuration

Usage Guideline Use the set command to set the DSCP field, COS field, or precedence field of the matched packet to a new value. Use set internal-cos command to directly assign the CoS queue to the matched packet.

Configure multiple set commands for a class if they are not conflicting. For example, precedence and dscp cannot be set at the same time.

The set dscp command will not affect the CoS queue selection. The set internal-cos command will not alter the CoS field of the outgoing packet.

If the policer is applied as the policy for the traffic class, the set actions configured by this command will be applied to the conforming packets. They will not be applied to the exceeding packet and the violating packet.

Example In the following example, the policy map policy1 is configured with the policy for the class1 class. The packets that are included in the class1 class will be set to a

DSCP of 10 and policed by a singe rate policer with an average rate set to128 Kbits per second and the normal burst size set to 256 Kbytes.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)# police 128 256 exceed-action set-dscp-transmit 3
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

Verify the settings by entering the **show policy-map** command.

set as-path

Use this command to modify an autonomous system path for BGP routes. To delete an entry, use the **no** form of this command.

set as-path prepend *AS-NUMBER-LIST*

no set as-path prepend *AS-NUMBER-LIST*

Syntax Description	
AS-NUMBER-LIST	Appends the string following the keyword prepended to the autonomous systempath of the route, that is matched by the route map. Applies to inbound and outbound BGP route maps. It can specify an AS number or a list of AS number. AS number <1-4294967295> or <1.0-65535.65535>

Default Disabled

Command Mode Route-map configuration

Usage Guideline The only global BGP metric available to influence the best path selection is the autonomous system path length. By varying the length of the autonomous system path, a BGP speaker can influence the best path selection to a peer further away.

The **set as-path prepen**d variation allows an arbitrary autonomous system path string to be prepended to BGP routes. Usually the local autonomous system number is prepended multiple times, increasing the autonomous system path length.

When as-path is not modified by the route map, by default, the local AS will be prepended in the access list.

Example This example shows how to set the as-path list 1, 10, 100, 200 with route map entry myPolicy:

```
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)#set as-path prepend 1 10 100 200
```

Verify the settings by entering the **show route-map** command.

set community

Use this command to set the BGP communities attribute, to delete an entry, use the **no** form of this command.

set community { *COMMUNITY-NUMBER* **[additive] |** *WELL-KNOWN-COMMUNITY* **[additive] | none }**

no set community {*COMMUNITY-NUMBER* **[additive] |** *WELL-KNOWN-COMMUNITY* **[additive] }**

Syntax Description	
COMMUNITY-NUMBER	The community number value. It is presented in a “AA:NN” format, and the AA and the NN both are numbers from 0 to 65535.
WELL-KNOWN-COMMUNITY	(Optional) Well known communities can be specified by using the following keywords: **internet** : Specifies routes not to be advertised to the Internet. **local-AS**: Specifies routes not to be advertised peers outside of the AS including sub-AS. **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.
additive	(Optional) Adds the community to the already existing communities.
none	Removes the community attribute from the prefixes that pass the route map.

Default Disabled

Command Mode Route-map configuration

Usage Guideline BGP community exchange is not enabled by default. It is enabled on a per-neighbor basis with the neighbor send-community command.

The community will be sent out in the BGP packet only when set community is specified in the route map, and if all match criteria are met, all set actions are performed.

If additive is not specified, the user-defined communities in the route will be replaced.

User-defined community is transitive, Well-known community is not-transitive.

This command is useful for routes received from EBGP and to be transmitted to IBGP.

Example This example shows how to set a community (0:1) to the route map entry with name myPolicy:

```
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# set community 0:1
Switch(config-route-map)#
```

Verify the settings by entering the **show route-map** command.

set default interface

Use the command in route-map configuration mode to set the interface to route the packets that pass a match clause of a route map and there is no route for the packets. To remove the setting, use the no form of the command to remove the setting.

set default interface INTERFACE-NAME

no set default interface [INTERFACE-NAME]

Syntax Description	
*INTERFACE-**NAME***	Specify the interface to route the packet.

Default Not configured

Command Mode Route-map configuration

Usage Guideline If other set clauses for policy based routing are used with the command, they will be evaluated based on the following ordering:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

With this ordering, the set next-hop clauses and the set interface clauses will be evaluated before look up of the routing table. If route cannot be found for the packets, the **set ip default next-hop** and **set default interface** command will be evaluated.

Examples The following example sends packets with the destination IP address specified by access list name IPACL-01 and for which the software has no explicit route to the destination are output to vlan200:

```
Switch(config)#route-map example permit 10
Switch(config-route-map)# match ip address IPACL_01
Switch(config-route-map)# set default interface vlan200
Switch(config-route-map)# exit
Switch(config)#interface vlan100
Switch(config-if)#ip policy route-map example
Switch(config-if)#exit
Switch(config)#
```

You can verify your settings by entering the **show route-map** privileged EXEC command.

set ip next-hop

Use this command to set the next-hop to route the packets that pass a match clause of a route map. Use the no command to remove the setting.

set ip next-hop *IP-ADDRESS*

no set ip next-hop [*IP-ADDRESS***]**

Syntax Description	
IP-ADDRESS	Specify the next hop to route the packet. The next hop must be an adjacent router.

Default Not configured

Command Mode Route-map configuration

Usage Guideline You can use this command to set the next hop to route the packets that pass a match clause of a route map.

If other set clauses for policy based routing are used with the command,they will be evaluated based on the following ordering:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

With this ordering, the set next-hops clauses and the set interface clauses will be evaluated before look up of the routing table. If route cannot be found for the packets, the set ip default next-hop and set default interface command will be evaluated.

Example In the following example, PBR will change the next-hop setting when the source ip is 10.1.1.0/24 and vlan is vlan100. We want to set next-hop of this route entry to 120.1.2.2. The steps as follows:

At first, create an IP basic access list, named *Strict-Control* which permit prefix 10.1.1.0/24.

Secondly, create a route map, named *myPolicy* which define a match rule to associate ip address prefix-list to the previously created access list, *Strict-Control*.

Lastly, in Vlan Interface configuration mode set the conditionally redistributed to previously created route-map, *myPolicy*.

```
Switch(config)# ip access-list Strict-Control
Switch(config-ip-acl)# permit 10.1.1.0 255.255.255.0 any
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
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)# exit
Switch(config)# interface vlan100
Switch(config-router)# ip policy route-map myPolicy
```

You can verify your settings by entering the **show route-map** privileged EXEC command.

set ip precedence

Use the **set ip precedence** command in route-map configuration mode to set the precedence value in the IP header. Use the no form of the command to remove the setting.

set ip precedence {*NUMBER* | *NAME*}

no set ip precedence {*NUMBER* | *NAME*}

Syntax Description

NUMBER | *NAME* — Specify one of the following numbers or names to set the precedence value in the IP header:

Number	Name
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

Default Not configured

Command Mode Route-map configuration

Usage Guideline Use the command to set the precedence value in the IP header.

The precedence can be set using either a number or the corresponding name.

Example The following example sets the IP Precedence value to 5 (critical) for packets that pass the route map match.

```
Switch(config)#route-map example permit 10
Switch(config-route-map)# match ip address IPACL_01
Switch(config-route-map)# set ip precedence 5
Switch(config-route-map)# exit
Switch(config)#interface vlan100
Switch(config-if)#ip policy route-map example
Switch(config-if)#exit
Switch(config)#
```

You can verify your settings by entering the **show route-map** privileged EXEC command.

set interface

Use the command in route-map configuration mode to set the interface to route the packets that pass a match clause of a route map. To remove the setting, use the **no** form of the command to remove the setting.

set interface *INTERFACE-NAME*

no set interface [*INTERFACE-NAME***]**

Syntax Description	
INTERFACE-NAME	Specify the interface to route the packet.

Default Not configured

Command Mode Route-map configuration

Usage Guideline If other set clauses for policy based routing are used with the command, they will be evaluated based on the following ordering:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

With this ordering, the set next-hop clauses and the set interface clauses will be evaluated before look up of the routing table. If route cannot be found for the packets, the set ip default next-hop and set default interface command will be evaluated.

Example The following example sends packets with the destination IP address specified by access list name IPACL-01 are output to Vlan200.

```
Switch(config)#route-map example permit 10
Switch(config-route-map)# match ip address IPACL-01
Switch(config-route-map)# set interface vlan200
Switch(config-route-map)# exit
Switch(config)#interface vlan100
Switch(config-if)#ip policy route-map example
Switch(config-if)#exit
Switch(config)#
```

You can verify your settings by entering the **show route-map privileged** *EXEC* command.

set ipv6 default next-hop

Use the command in route-map configuration mode to set the next hop to route the packets that pass a match clause of a route map and there is no route for the packets. To remove the setting, use the **no** form of the command to remove the setting.

set ipv6 default next-hop *IPv6-ADDRESS*

no set ipv6 default next-hop [*IPv6-ADDRESS***]**

Syntax Description	
IPv6-ADDRESS	Specify the next hop to route the packet. The next hop must be an adjacent router.

Default Not configured

Command Mode Route-map configuration

Usage Guideline You can use this command to set the next hop to route the packets that pass a match clause of a route map.

If other set clauses for policy based routing are used with the command, they will be evaluated based on the following ordering:

1. **set ipv6 next-hop**
2. **set interface**
3. **set ipv6 default next-hop**
4. **set default interface**

With this ordering, the set interface clauses and the set interface clauses will be evaluated before look up of the routing table. If route cannot be found for the packets, the set ip default next-hop and set default interface command will be evaluated.

Examples In the following example, PBR will change the next-hop setting when the source ip is 2000::/16 and vlan is vlan100 and can not found the destination address in routing table.

We want to set next-hop of this route entry to 100::BEAE:C5FF:FE9A. The steps as follows:

At first, create an IP basic access list, named *Strict-Control* which permit prefix 2000::/16

Secondly, create a route map, named *myPolicy* which define a match rule to associate ip address prefix-list to the previously created access list, *Strict-Control*.

Lastly, in Vlan Interface configuration mode set the conditionally redistributed to previously created route-map, *myPolicy*.

```
Switch(config)# ipv6 access-list extended Strict-Control
Switch(config-ip-acl)# permit 2000::3:4 ffff::0 any
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match ipv6 address Strict-Control
Switch(config-route-map)# set ipv6 default next-hop 100::BEAE:C5FF:FE9A
Switch(config-route-map)# exit
Switch(config)# interface vlan100
Switch(config-router)# ip policy route-map myPolicy
```

You can verify your settings by entering the **show route-map** privileged EXEC command.

set ip default next-hop

Use the command in route-map configuration mode to set the next hop to route the packets that pass a match clause of a route map and there is no route for the packets. To remove the setting, use the **no** form of the command to remove the setting.

set ip default next-hop *IP-ADDRESS*

no set default next-hop [*IP-ADDRESS***]**

Syntax Description	
IP-ADDRESS	Specify the next hop to route the packet. the next hop must be an adjacent router.

Default Not configured

Command Mode Route-map configuration

Usage Guideline If other set clauses for policy based routing are used with the command, they will be evaluated based on the following ordering:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

With this ordering, the set next-hop clauses and the set interface clauses will be evaluated before look up of the routing table. If route cannot be found for the packets, the set ip default next-hop and set default interface command will be evaluated.

Example In the following example, PBR will change the next-hop setting when the source ip is 10.1.1.0/24 ,vlan is vlan100 and can not found the destination address in routing table. We want to set next-hop of this route entry to 120.1.2.2. The steps as follows:

At first, create an IP basic access list, named Strict-Control which permit prefix 10.1.1.0/24.

Secondly, create a route map, named *myPolicy* which define a match rule to associate ip address prefix-list to the previously created access list, Strict-Control.

Lastly, in Vlan Interface configuration mode set the conditionally redistributed to previously created route-map, *myPolicy*.

```
Switch(config)# ip access-list Strict-Control
Switch(config-ip-acl)# permit 10.1.1.0 255.255.255.0 any
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match ip address Strict-Control
Switch(config-route-map)# set ip default next-hop 120.1.2.2
Switch(config-route-map)# exit
Switch(config)# interface vlan100
Switch(config-router)# ip policy route-map myPolicy
```

You can verify your settings by entering the **show route-map privileged** *EXEC* command.

set ipv6 next-hop

Use this command to set the next-hop to route the packets that pass a match clause of a route map. Use the no command to remove the setting.

set ipv6 next-hop *IPv6-ADDRESS*

no set ipv6 next-hop [*IPv6-ADDRESS***]**

Syntax Description	
IPv6-ADDRESS	Specify the next hop to route the packet. The next hop must be an adjacent router.

Default Not configured

Command Mode Route-map configuration

Usage Guideline If other set clauses for policy based routing are used with the command, they will be evaluated based on the following ordering:

1. **set ipv6 next-hop**
2. **set interface**
3. **set ipv6 default next-hop**
4. **set default interface**

With this ordering, the set next-hop clauses and the set interface clauses will be evaluated before look up of the routing table. If route cannot be found for the packets, the set ip default next-hop and set default interface command will be evaluated.

Example In the following example, PBR will change the next-hop setting when the source ip is 2000::/16 and vlan is vlan100. We want to set next-hop of this route entry to 100::BEAE:C5FF:FE9A. The steps as follows:

At first, create an IP basic access list, named Strict-Control which permit prefix 2000::/16

Secondly, create a route map, named myPolicy which define a match rule to associate ip address prefix-list to the previously created access list, Strict-Control.

Lastly, in Vlan Interface configuration mode set the conditionally redistributed to previously created route-map, *myPolicy*.

```
Switch(config)# ipv6 access-list extended Strict-Control
Switch(config-ip-acl)# permit 2000::3:4 ffff::0 any
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match ipv6 address Strict-Control
Switch(config-route-map)# set ipv6 next-hop 100::BEAE:C5FF:FE9A
Switch(config-route-map)# exit
Switch(config)# interface vlan100
Switch(config-router)# ip policy route-map myPolicy
```

You can verify your settings by entering the **show route-map** privileged EXEC command.

set default interface

Use the command in route-map configuration mode to set the interface to route the packets that pass a match clause of a route map and there is no route for the packets. To remove the setting, use the **no** form of the command to remove the setting.

set default interface *INTERFACE-NAME*

no set default interface [*INTERFACE-NAME***]**

Syntax Description	
INTERFACE-NAME	Specify the interface to route the packet.

Default Not configured

Command Mode Route-map configuration

Usage Guideline If other set clauses for policy based routing are used with the command, they will be evaluated based on the following ordering:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

With this ordering, the set next-hop clauses and the set interface clauses will be evaluated before look up of the routing table. If route cannot be found for the packets, the set ip default next-hop and set default interface command will be evaluated.

Example The following example sends packets with the destination IP address specified by access list name IPACL-01 and for which the software has no explicit route to the destination are output to vlan200:

```
Switch(config)#route-map example permit 10
Switch(config-route-map)# match ip address IPACL_01
Switch(config-route-map)# set default interface vlan200
Switch(config-route-map)# exit
Switch(config)#interface vlan100
Switch(config-if)#ip policy route-map example
Switch(config-if)#exit
Switch(config)#
```

set origin

To set the BGP origin code, use the set origin command in route-map configuration mode. To delete an entry, use the no form of this command.

set origin {igp | **egp** | **incomplete}**

no set origin {igp | **egp** | **incomplete}**

Syntax None

Default Disabled

origin: based on the route in the main IP routing table.

Command Mode Route-map configuration

Usage Guideline Use the route-map global configuration command, and the match and set route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each route-map command has a list of match and set commands associated with it. The match—the conditions under which redistribution is allowed for the current route-map command. The set—the particular redistribution actions to perform if the criteria enforced by the match commands are met. The no route-map command deletes the route map.

The set route-map configuration commands specify the redistribution set actions to be performed when all of the match criteria of a route map are met. When all match criteria are met, all set actions are performed.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, signifying that the prefix was originated from information learned from an interior gateway protocol.
- EGP, signifying that the prefix originated from the EGP protocol, which BGP replaced.
- INCOMPLETE, meaning the prefix originated from some unknown source.

Example This example shows how to set the origin of routes, that pass the route map named myPolicy, to EGP.

```
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match as-path PATH_ACL
Switch(config-route-map)# set origin egp
```

Verify the settings by entering the **show route-map** command.

set weight

To specify the BGP weight for the routing table, use the **set weight** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set weight *NUMBER*

no set weight *NUMBER*

Syntax Description	
NUMBER	Weight value. It can be an integer ranging from 0 to 65535.

Default Disabled

Command Mode Route-map configuration

Usage Guideline The implemented weight is based on the first matched autonomous system path. Weights indicated when an autonomous system path is matched override the weights assigned by global neighbor commands. In other words, the weights assigned with the set weight route-map configuration command override the weights assigned using the neighbor weight command.

Example This example shows how to add the policy routing entry with name myPolicy and set the weight to 30 when it match the as-path access list with PATH_ACL:

```
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match as-path PATH_ACL
Switch(config-route-map)# set weight 30
```

Verify the settings by entering the **show route-map** command.

sflow

Use the sflow command to enable sFlow functions. Use the no form of this command to disable sFlow functions.

sflow

no sflow

Syntax None

Default sFlow is disabled by default.

Command Mode Global configuration mode.

Usage Guideline When sFlow is disabled, Receivers stop to countdown and do not send sFlow datagrams. User can still configure sFlow objects.

Example This example shows how to enable sFlow functions.

```
switch(config)# sflow
```

sflow receiver

Use the **sflow receiver** command to configure a Receiver for the sFlow agent. Receivers cannot be added to or removed from the sFlow agent. Use the **no** form of this command to reset one Receiver or all Receivers to the default settings.

sflow receiver INDEX **[owner** NAME**] [expiry {**SECONDS **| infinite}] [max-datagram-size** SIZE**] [host {**IP-ADDRESS|IPV6-ADDRESS**}] [udp-port** PORT**]**

no sflow receiver [INDEX**]**

Syntax

INDEX	Index of the Receivers. The maximum number is project dependent.
owner *NAME*	(Optional)Specify the owner name of the Receiver. It can accept up to 32 characters. The syntax is general string that does not allow space. The user can not directly configure the owner as an empty string.
expiry *SECONDS*	(Optional)Specify the expiration time for the entry. The parameter of the entry will be reset when the timer expired. The range is from 0 to 2000000. The user cannot directly configure the expiry timer as 0.
infinite	(Optional)The entry will not be expired.
max-datagram-size *SIZE*	(Optional)Specify the maximum number of data bytes of a single sFlow datagram. The valid range is from 700 to 1400.
host *IP-ADDRESS*	(Optional)The IPv4 address of the remote sFlow collector.
IPV6-ADDRESS	(Optional)The IPv6 address of the remote sFlow collector. It does not support IPv6 link-local address.
udp-port *PORT*	(Optional)The UDP port of the remote sFlow collector. The default is 6343. The range is from 1 to 65535.

Default

The default owner name is an empty string

Expiry timer is 0 second

Max datagram size is 1400 bytes

Receiver IP address is 0.0.0.0

UDP port number is 6343

Command Mode

Global configuration mode

Usage Guideline

The sFlow agent has a fix number of Receivers distinguished by INDEX. They are created in reset state by system and cannot be removed.

The user must configure the owner of an entry before configuring other parameters of the entry. The owner of an entry can only be configured when the entry is in reset state. The user can not configure the owner name as an empty

string. Once the owner is configured, it cannot be changed directly. It can only be reset by the **no sflow receiver** command.

Use the **no sflow receiver** command to reset the Receiver.

When a Receiver expired, the Receiver is disabled and the Receiver entry will be reset to the default settings. The expiration timer starts to count down when its value is configured.

The user cannot configure the expiry timer as 0.

Example

This example shows how to configure the Receiver of INDEX 1 with owner name as collector1, TIMEOUT as 86400 seconds, SIZE as 1400 bytes,

sFlow collector's IP-ADDRESS as 10.1.1.2 and PORT as 6343.

```
switch(config)# sflow receiver 1 owner collector1 expiry 86400 max-datagram-
size 1400 host 10.1.1.2 udp-port 6343
```

sflow sampler

Use the **sflow sampler** command to create/configure a Sampler for the sFlow agent. Use the **no** form of this command to delete one Sampler or all Samplers.

sflow sampler INSTANCE **[receiver** RECEIVER**][sampling-rate** RATE**][max-header-size** SIZE**]**

no sflow sampler [INSTANCE**]**

Syntax

INSTANCE	The instance index if multiple Samplers are associated with one interface. The valid range is from 1 to 65535.
receiver *RECEIVER*	(Optional)The Receiver's *INDEX* for this Sampler. If not specified, the value is 0. The user can not configure the value to 0. The maximum number is project dependent.
sampling-rate *RATE*	(Optional)The rate for packet sampling. The range is from 0 to 65536. 0 means disable. If not specified, the default value is 0.
max-header-size *SIZE*	(Optional)The maximum number of bytes that should be copied from sampled packets. The range is from 18 to 256. If not specified, the default value is 128.

Default

No Sampler is created.

Command Mode

Interface configuration mode

Usage Guideline

The command is available for physical port interface configuration.

A sampler can only be configured on one interface. It cannot be associated with multiple interfaces.

Use this command without keywords to create a default Sampler or to reset an existing Sampler to default values. Use the **no** form of this command with INSTANCE to delete one Sampler. Use the **no** form of this command without INSTANCE to delete all Samplers.

The user can only specify a Receiver that has its owner name setup. If the Receiver associated with the sampler has its owner name reset, the sampler will be reset to the default setting. The Receiver ID of a default sampler is 0.

Set sampling rate to N will cause the system to sample one packet for every N packets arriving on the monitored interface. The sampled packet is sent to the sFlow Receiver. Setting the sampling rate to 0 will disable the sampling. The granularity of the sampling rate is project dependent.

An interface can be configured with multiple samplers. If multiple samplers are configured, the configured sampling rate can be different. However, the sampling rate of all other samplers must be multiples in power of 2 of the minimal sampling rate.

Example This example shows how to create/configure the Sampler of INSTANCE 1 with RECEIVER as 1, RATE as 1024 and SIZE as 128 bytes.

```
switch(config-if)# sflow sampler 1 receiver 1 sampling-rate 1024 max-header-size 128
```

sflow poller

Use the **sflow poller** command to create/configure a Poller for the sFlow agent. Use the **no** form of this command to delete one Poller or all Pollers.

sflow poller INSTANCE **[receiver** RECEIVER**][interval** SECONDS**]**

no sflow poller [INSTANCE**]**

Syntax

INSTANCE	The instance index if multiple Pollers are associated with one interface. The range is from 1 to 65535.
receiver *RECEIVER*	(Optional)The Receiver's *INDEX* for this Poller. If not specified, the value is 0. The user can not configure the value to 0. The maximum number is project dependent.
Interval *SECONDS*	(Optional)The maximum number of seconds between successive polling samples. The range is from 0 to 120. 0 means disable. If not specified, the default is 0.

Default

No Poller is created.

Command Mode

Interface configuration mode.

Usage Guideline

The command is available for physical port interface configuration.

A Poller can only be configured on one interface. It cannot be associated with multiple interfaces.

Use this command without keywords to create a default Poller or to reset an existing Poller to default values. Use the **no** form of this command with INSTANCE to delete one Poller. Use the **no** form of this command without INSTANCE to delete all Pollers.

The user can only specify a Receiver that has its owner name setup. If the Receiver associated with the Poller has its owner name is reset, the Poller will be reset to the default setting.

Setting the polling interval to 0 disables the polling.An interface can be configured with multiple Pollers.

Example

This example shows how to create/configure the Poller of INSTANCE 1 with RECEIVER as 1, and INTERVAL as 20 seconds.

```
switch(config-if)# sflow poller 1 receiver 1 interval 20
```

show aaa

Use **show aaa** to display the login/enable method list for all applications.

show aaa [login | **enable] [console** | **telnet** | **http | ssh] [brief]**

Syntax Description	
login	(Optional) Displays the login authentication information
enable	(Optional) Displays the enable authentication information.
console	(Optional) Displays the console authentication information.
telnet	(Optional) Displays the telnet authentication information.
http	(Optional) Displays the http authentication information.
ssh	(Optional) Displays the ssh authentication information.
brief	(Optional) Displays the brief format of the authentication type (skip information about the detailed server list of the associating method list).

Default None

Command Mode Privilege EXEC or any configuration mode at privilege level 15

Usage Guideline Display the login/enable method list for all applications. If the brief option is specified, the detailed server list of the associating method list will be skipped,

Examples This example shows how to display the login/enable method list for all applications.

```
DGS-6604:15#show aaa

Console Session:
  Login  authentication:
    Local Authentication: yes
  Enable authentication:
    Group Name: serverlist1
    Local Authentication: no
      IP Address      Protocol Port  Timeout Retransmit Key
      --------------- -------- ----- ------- ---------- ------------
      122.248.150.251 RADIUS   1812  5       2          **********

Telnet Session:
  Login  authentication:
    Group Name: serverlist1
    Local Authentication: no
      IP Address      Protocol Port  Timeout Retransmit Key
      --------------- -------- ----- ------- ---------- ------------
      122.248.150.251 RADIUS   1812  5       2          **********
  Enable authentication:
    Local Authentication: yes

Ssh Session:
  Login  authentication:
    Group Name: serverlist1
    Local Authentication: no
      IP Address      Protocol Port  Timeout Retransmit Key
      --------------- -------- ----- ------- ---------- ------------
      122.248.150.251 RADIUS   1812  5       2          **********
  Enable authentication:
    Local Authentication: yes

Http Session:
  Login  authentication:
    Local Authentication: yes
  Enable authentication:
    Local Authentication: yes
DGS-6604:15#
```

The following example displays brief information for authentication:

```
DGS-6604:15#show aaa brief
Application     Method  Server group                    Local
--------------- ------- ------------------------------- ----------
console         login                                   yes
console         enable  serverlist1                     no
telnet          login   serverlist1                     no
telnet          enable                                  yes
ssh             login   serverlist1                     no
ssh             enable                                  yes
http            login                                   yes
http            enable                                  yes
DGS-6604:15#
```

The following example displays brief information for enable authentication:

```
DGS-6604:15#show aaa enable brief
Application     Method  Server group                    Local
--------------- ------- ------------------------------- ----------
console         enable  serverlist1                     no
telnet          enable                                  yes
ssh             enable                                  yes
http            enable                                  yes
```

The following example displays brief information for enable authentication and the telnet application:

```
DGS-6604:15#show aaa enable telnet brief
Application     Method  Server group                    Local
--------------- ------- ------------------------------- ----------
telnet          enable                                  yes
DGS-6604:15#
```

The following example displays brief information for authentication and the console application:

```
DGS-6604:15#show aaa console brief
Application     Method  Server group                    Local
--------------- ------- ------------------------------- ----------
console         login                                   yes
console         enable  serverlist1                     no
DGS-6604:15#
```

show aaa group server

Use this command **show aaa group server** to display the authentication servers by group name or the authentication servers for all groups.

show aaa group server [*GROUP-NAME***]**

Syntax Description	
GROUP-NAME	(Optional) Specifies the name of the server method list to be displayed.The valid length for server-group is 1 to 16.

Default None

Command Mode Privilege EXEC or any configuration mode at privilege level 15

Usage Guideline Use this command to display the authentication servers by specifying the name (*GROUP-NAME*) of the group server list.

To see the servers for all groups, do not specify *GROUP-NAME*.

Examples This example shows how to display all the authentication server groups:

```
Switch:15#show aaa group server

Group Name         IP Address      Protocol Port  Timeout Retransmit Key
------------------ --------------- -------- ----- ------- ---------- ----------
serverlist1        122.248.150.251 RADIUS   1812  5       2          **********
serverlist1        122.248.150.100 RADIUS   1812  5       2          **********
serverlist1        122.248.150.11  RADIUS   1812  5       2          no-encrypt
serverlist2        100.1.1.1       TACACS   49    5       2
serverlist2        100.1.1.2       TACACS   49    5       2
serverlist2        100.1.1.12      TACACS   49    5       2
Switch:15#
```

This example shows how to display an authentication server group named authserv:

```
Switch:15#show aaa group server authserv
Group Name         IP Address      Protocol Port  Timeout Retransmit Key
------------------ --------------- -------- ----- ------- ---------- ----------
authserv           10.1.1.1        XTACACS  49    5       2
authserv           20.1.1.1        RADIUS   1812  5       2          **********
authserv           20.1.1.2        RADIUS   1812  5       2          no-encrypt
Switch:15#
```

show access-group

Use this command to display how the mac, ip and ipv6 access-lists are applied to interfaces.

show access-group [interface *INTERFACE-ID* **] [ip [** *NAME* **] | mac [** *NAME* **] | ipv6 [** *NAME* **]]**

Syntax Description	
interface *INTERFACE-ID*	(Optional) Specifies the interface to be displayed. If not specified, the access-groups for all interfaces will be displayed.
ip	(Optional) Specifies that only the ip access group on the specified interface(s) will be displayed.
mac	(Optional) Specifies that only the mac access group on the specified interface(s) will be displayed.
ipv6	Optional) Specifies that only the ipv6 access group on the specified interface(s) will be displayed.
NAME	(Optional) The name of the access-list (mac, ip, ipv6) to be displayed.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Since there is both an **ip extended access-list** and an **ip access-lis**t, use the **access-list** *NAME* to distinguish them.

Example This example shows how the IP access-list is applied to all of the interfaces.

```
Switch# show access-group
eth3.1
  Inbound mac access-list : simple-mac-acl
  Inbound ip access-list  : simple-ip-acl
  Inbound ipv6 access-list : ip6-control
eth3.2
  Inbound mac access-list : rd-mac-acl
  Inbound ip access-list  : rd-ip-acl
  Inbound ipv6 access-list : N/A
```

show access-list

Use this command to display the access-list configuration.

show access-list [ip *NAME* **| mac** *NAME* **| ipv6** *NAME***]**

Syntax Description	
ip	(Optional) Specifies to display a listing for all ip access-lists.
mac	(Optional) Specifies to display a listing for all mac access-lists.
ipv6	(Optional) Specifies to display a listing for all ipv6 access-lists.
NAME	Specifies to display the content of the access-list identified by this *NAME* string. Up to 32 characters are allowed.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline The detailed content for an access list is only shown for a specific access-list by using the *NAME* argument to identify it.

Examples This example provides a listing for all access lists.

```
Switch#show access-list
access-list name                  access-list type
------------------------------- ----------------
rd-mac-acl                            mac ext-acl
simple-ip-aclip                        ip acl
rd-ip-acl                              ip acl
simple-rd-aclip                     ip ext-acl
ip6-acl                            ipv6 ext-acl
Total Entries : 5
Switch#
```

This example shows the content for IP access-list *R&D.*

```
Switch# show access-list ip R&D
10 permit tcp any 10.20.0.0 255.255.0.0
20 permit tcp any host 10.100.1.2
30 permit icmp any any
```

show arp

Use the **show arp** command to display the Address Resolution Protocol (ARP) cache.

show arp [*ARP-MODE*] [*IP-ADDRESS* [*/ MASK*]] [*INTERFACE-ID*]

Syntax Description	
ARP-MODE	(Optional) Displays the entries that are in a specific ARP mode. This argument can be replaced by one of the following keywords: **dynamic**—Displays only dynamic ARP entries. A dynamic ARP entry is learned through an ARP request and completed with the MAC address of the external host. **static**—Displays only static ARP entries. A static ARP entry is a statically configured (permanent) ARP.
IP-ADDRESS *[/MASK]*	(Optional) Displays the entries associated with a specific host or network entry that is associated with an external host.
INTERFACE-ID	(Optional) Displays only the ARP table entries associated with this interface such as, for example, a VLAN interface such as vlan100.

Default None

Command Mode User EXEC mode or any configuration mode

Usage Guideline ARP establishes correspondences between network addresses (an IP address, for example) and LAN hardware addresses (Ethernet addresses). A dynamic record of each correspondence is kept in a cache for a predetermined amount of time and then discarded. The predetermined amount of time can be changed using the **arp timeout** command. If no arp mode argument is specified, then all of the arp entries are displayed.

The user can select to display a specific ARP entry, all ARP entries, dynamic entries, static entries, or entries associated with an IP interface.

Example This example shows how to display the ARP cache. The field of IP Interface is indicated with the Interface ID.

```
Switch#show arp
Address                  Hardware Addr       IP Interface     Type
-------------------------------------------------------------------
10.108.42.112         00-00-a7-10-4b-af      vlan100          Static
10.108.42.114         00-00-a7-10-85-9b      vlan200          Dynamic
10.108.42.121         00-00-a7-10-68-cd      vlan300          Dynamic
Total Entries: 3
Switch#
```

show boot

Use this command to display which is the next boot configuration and which is the next boot image file.

show boot

Syntax None

Default None

Command Mode User EXEC

Usage Guideline None

Example The following example shows the display information for the system boot information:

```
Switch# show boot
Boot loader version 1.00.004
Boot image: flash:\switch-image1.had, flash:\switch-image2.had
Boot config: flash:\switch-config
Switch#
```

show channel-group

Use this command to display the information of channel groups.

show channel-group [[channel [*CHANNEL-NO*] [detail | neighbor | protocol]] | load-balance | sys-id]

Syntax Description	
CHANNEL-NO	Channel group ID.
channel	(Optional) Display information for specified port-channels.
detail	(Optional) Display detailed channel group information.
neighbor	(Optional) Display neighbor information.
protocol	(Optional) Display the protocol (static or LACP) that is being used in the channel group.
load-balance	(Optional) Display the load balance information.
sys-id	(Optional) Display the system identifier that is being used by LACP.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use the keyword **channel** to display the port-channel information. If the arguments: **detail**, **neighbor** or **protocol** are not specified, then the switch will display detailed information for the specified port-channels.

If the port-channel number is not specified, then all port-channels will be displayed.

If the arguments: **channel**, **load-balance** and **sys-id** are specified for the **show channel-group** command, only summary channel-group information will be shown.

Examples This example shows how to display the neighbor information for port-channel 3.

```
Switch> show channel-group channel 3 neighbor
S - Device is requesting Slow LACPDUs, F - Device is requesting Fast LACPDUs,
A - Device is in Active mode,          P - Device is in Passive mode,

Partner                    Partner    Partner    Partner
Port       System ID                  PortNo    Flags      Port_Pri.
-----------------------------------------------------------------------
eth3.1    32768,00-07-eb-49-5e-80    12        SP         32768
eth3.2    32768,00-07-eb-49-5e-80    13        SP         32768

Switch>
```

This example shows how to display the detailed information of all port-channels.

```
Switch> show channel-group channel detail
S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDU
A - Device is in active mode.        P - Device is in passive mode.

LACP state:
bndl: Port is attached to an aggregator and bundled with other ports.
hot-sby:  Port is in a hot-standby state.
indep:    Port is in an independent state(not bundled but able to switch
data
            traffic)
down:     Port is down.

Channel Group 1
Member Ports: 2, Maxports = 16, Protocol: LACP
                     LACP          Port        Port
Port          Flags  State         Priority    Number
-----------------------------------------------
eth3.10       SA     bndl          32768        10
eth3.11       SA     bndl          32768        11

Channel Group 2
Member Ports: 2, Maxports = 8, Protocol: Static
            LACP
Port        State
-----------------
eth3.8      bndl
eth3.9      down

Switch>
```

This example shows how to display the protocol information for all port-channels.

```
Switch> show channel-group channel protocol

Group          Protocol
------------------------
1               LACP
2               Static

Total Entries: 2
Switch>
```

This example shows how to display the load balance information for all channel groups.

```
Switch> show channel-group load-balance
load-balance algorithm: src-dst-mac
Switch>
```

This example shows how to display the system identifier information

```
Switch> show channel-group sys-id
32765,00-02-4b-29-3a-00
Switch>
```

This example shows how to display the information of all the port-channels in brief format.

```
Switch> show channel-group
Group          Protocol
-----------------------
1               LACP
2               Static

Total Entries: 2
load-balance algorithm: src-dst-mac
system-ID: 32765,00-02-4b-29-3a-00
```

show class-map

Use this command to display the class map configuration.

show class-map [*NAME***]**

Syntax Description	
NAME	(Optional) Name of the class map. The class map name can be a maximum of 32 alphanumeric characters.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline The user can use the **show class-map** command to display all class maps and their matching criteria. If the optional *NAME* argument is entered, the specified class map and its matching criteria will be displayed.

Example In the following example, two class maps are defined. Packets that match access list acl_home_user belong to class c3, IP packets belong to class c2. The output from the show class-map command shows the default class, class-default and two defined class maps.

```
Switch# show class-map
Class Map match-any c2
  match protocol ip
Class Map match-any c3
  match access-list acl_home_user
Total Entries: 2
Switch#
```

show clock

Use this command to display the time and date information.

show clock

Syntax None

Default None

Command Mode EXEC mode or any configuration mode

Usage Guideline This command will also indicate the clock source. The clock source can be one of "No Time Source" or "SNTP".

Example The following example shows how to display the current time:

```
Switch> show clock
Current Time Source  : No Time Source
Current Time         : 19:14:16, 2010-12-06
Time Zone            : UTC -08:00
Daylight Saving Time : Recurring
Offset in Minutes    : 60
   Recurring From : Apr 2nd Tue 15:00
                To : Oct 2nd Wed 15:30
Switch>
```

show cpu-protect safeguard

Use this command to display the settings and status of Safeguard Engine.

show cpu-protect safeguard

Syntax Description none

Default none

Command Mode Privileged EXEC mode

Usage Guideline The command **show cpu-protect safeguard** is used to display the settings and status of Safeguard Engine.

Example The following example shows how to display the settings and current status of Safeguard Engine.

```
Switch# show cpu-protect safeguard

Safeguard Engine State     : Disabled
Safeguard Engine Status    : Normal

Utilization Thresholds:
Rising          : 50%
Falling         : 20%

Switch#
```

show cpu-protect type

Use this command to show the rate-limit and statistics of CPU protection

show cpu-protect type { *PROTOCOL-NAME* [*UNIT-ID*] | **unit** *UNIT-ID* }

Syntax Description

PROTOCOL-NAME [*UNIT-ID*]	The configured rate-limit and statistics of the specified protocol on CM-Card and all existing IO-Cards will be displayed if the optional [*UNIT-ID*] is not specified. Otherwise, only the information on the specified unit id will be displayed.
unit *UNIT-ID*	Specify the unit id which you want to display the rate-limit configuration and statistics. For chassis system device, the unit ID is equal to blade ID (or slot ID).

Default none

Command Mode Privileged EXEC mode.

Usage Guideline Show configured rate limit and drop-count of Safeguard engine of specific group. These counters are counted by the software. There is probably deviation from the hardware received if the packets are dropped before sent to CPU.

Example The following example is a sample output of **show cpu-protect** type command. N/A means no rate-limit is applied to this protocol.

```
Switch# show cpu-protect type unit 1

Type                Pps       Total     Drop
------------------ --------- --------- ---------
stp                 300       20        0
gvrp                400       24        0
lacp                N/A       0         0
8021x               0         0         0
arp                 0         0         0
icmpv4              0         0         0
icmpv6-neighbor     0         0         0
icmpv6-other        0         0         0
pim                 0         0         0
rip                 0         0         0
ospf                0         0         0
!--- Output suppressed.

Switch#
```

The following example is a sample output of the **show cpu-protect** type arp command. The configured rate is 300 pps, and there exists one IO-card on slot 3.

```
Switch# show cpu-protect type arp
Type: arp
Pps : 300
Slot            Total     Drop
--------------  --------- ---------
1 (CM-card)     30        0
3               30        0
Switch#
```

show cpu-protect sub-interface

Use this command to show the rate-limit and statistics by sub-interface.

show cpu-protect sub-interface { manage | protocol | route } [*UNIT-ID***]**

Syntax Description	
UNIT-ID	(Optional) Specify the unit id, that you want, to display the rate limit configuration and statistics by sub-interface. For the chassis system device, the unit ID is equal to a blade ID (or slot ID).

Default none

Command Mode Privileged EXEC mode

Usage Guideline Show configured rate limit and drop-count of Safeguard engine of specific group. These counters are counted by the software. There is probably deviation from the hardware received if the packets are dropped before sent to CPU.

Example The following example is a sample output of the **show cpu-protect sub-interface manage** command. The configured rate is 300 packets per second, and there exists one IO-card on slot 3.

```
Switch# show cpu-protect sub-interface manage
Sub-Interface: manage
Pps : 300
Slot            Total     Drop
--------------  --------- ---------
1(CM-card)         50        0
3                  50        0
Switch#
```

The following is a sample output of the **show cpu-protect sub-interface protocol** command. The Pps is "N/A" which means no rate-limit is applied to route sub-interface.

```
Switch# show cpu-protect sub-interface protocol
Sub-Interface: protocol
Pps : N/A
Slot            Total     Drop
--------------  --------- ---------
1(CM-card)              0        0
3                       0        0
Switch#
```

show dos_prevention

Use this command to show DoS prevention status and related drop counters.

show dos_prevention

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Displays information about DoS prevention.

Example The following example shows the information of a DoS configuration example. User has configured to enable DoS on attacking type “Land Attack”, ”Blat Attack” and the action “Drop”, ”Log” are enabled. (Please note that **enable dos prevention** to block blat_attack may block the Syslog packets.)

The “Action” row shows users have enabled “Drop”, “Log” actions. The original received attacking packets of “Land Attack”, ”Blat Attack” will be dropped. Each packet dropped by DoS module will cause “Frame Count” increasing by 1. For every five minutes, DoS module will add one log to system log if any attacking packet is received in this interval.

```
Switch# Switch# show dos_prevention
DoS Prevention Information
Action: Drop Log
Frame Counts: 12345678
DoS Type                                    State
-------------------------------------------------
Land Attack                                 Enabled
Blat Attack                                 Enabled
Smurf Attack                                Disabled
TCP Null                                    Disabled
TCP Xmas                                    Disabled
TCP SYNFIN                                  Disabled
TCP SYN SrcPort Less Than 1024              Disabled
Switch#
```

show dot1v

Use the **show dot1v** command to display the setting for the configuration of VLAN protocols.

show dot1v { protocol-group [*GROUP-ID* **[, | -]] | interface [** *INTERFACE-ID* **[, | -]] }**

Syntax Description	
protocol-group	Show the protocol VLAN table entry information.
GROUP-ID	Specifies the dot1v protocol table entry number.
interface	Show the protocol VLAN group binding information of the ports.
INTERFACE-ID	Specifies the interface to display.
,	(Optional) Specifies a series of interfaces or GROUP-ID, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces or GROUP-ID. No space before and after the hyphen.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use the **show dot1v** command to display the current protocol VLAN status. Show the protocol VLAN group list table using the **show dot1v protocol-group** command. Show the protocol VLAN binding of the ports using the **show dot1v interface** command.

Example This example shows how to display protocol VLAN binding of interface ports 3.1 to 3.3.

```
Switch# show dot1v interface eth3.1-3.3
Interface        dot1v Group ID/Binding-VLAN
--------- ----------------------------------------
eth3.1            1/1
eth3.2            10/3000, 11/3001, 12/3002
eth3.3            2/100
Switch#
```

show dot1x

Use this command to display information about the: 802.1X state, configuration, statistics, diagnostics, session statistics, or authentication client.

show dot1x [interface *INTERFACE-ID* **] {auth-state | auth-configuration | statistics | diagnostics | session-statistics}**

Syntax Description	
interface *INTERFACE-ID*	(Optional) Specifies a port to display the authentication state, configuration, statistics, diagnostics, or session statistics. This option is only valid for a physical port interface.
auth-state	Display information of 802.1X state.
auth-configuration	Display information of 802.1X configuration.
statistics	Display information of 802.1X statistics.
diagnostics	Display information of 802.1X diagnostics.
session-statistics	Display information of 802.1X session statistics.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline If a port is not specified, then information for all ports will be displayed.

Examples This example shows how to display the authentication configuration for port eth4.1.

```
Switch#show dot1x interface eth4.1 auth-configuration

System Auth Control: Enabled
Authentication Protocol: Local

eth4.1
  PAE: Authenticator
  Control Direction: Both
  Port Control: Auto
  Quiet Period: 60
  Tx Period: 30
  Supp Timeout: 30
  Server Timeout: 30
  Max-req: 2
  Reauth Period: 3600
  Re-authentication: Disabled
  Authentication Mode: Host-based
  Guest VLAN: Disabled
  Forward 1x PDU: Disabled

Total Entries: 1
```

This example shows how to display the authentication statistics for port eth4.1.

```
Switch#show dot1x interface eth4.1 statistics

eth4.1
  EAPOL Frames RX: 0
  EAPOL Frames TX: 0
  EAPOL-Start Frames RX: 0
  EAPOL-Logoff Frames RX: 0
  EAPOL-Resp/Id Frames RX: 0
  EAPOL-Resp Frames RX: 0
  EAPOL-Req/Id Frames TX: 0
  EAPOL-Req Frames TX: 0
  Invalid EAPOL Frames RX: 0
  EAP-Length Error Frames RX: 0
  Last EAPOL Frame Version: 0
  Last EAPOL Frame Source: 00-00-00-00-00-00

Total Entries: 1
```

This example shows how to display the authentication diagnostics for port eth4.1.

```
Switch#show dot1x interface eth4.1 diagnostics

eth4.1
  EntersConnecting: 0
  EAP-LogoffsWhileConnecting: 0
  EntersAuthenticating: 0
  SuccessesWhileAuthenticating: 0
  TimeoutsWhileAuthenticating: 0
  FailsWhileAuthenticating: 0
  ReauthsWhileAuthenticating: 0
  EAP-StartsWhileAuthenticating: 0
  EAP-LogoffsWhileAuthenticating: 0
  ReauthsWhileAuthenticated: 0
  EAP-StartsWhileAuthenticated: 0
  EAP-LogoffsWhileAuthenticated: 0
  BackendResponses: 0
  BackendAccessChallenges: 0
  BackendNonNakResponsesFromSupplicant: 0
  BackendAuthSuccesses: 0
  BackendAuthFails: 0

Total Entries: 1
```

This example shows how to display the authentication session statistics for port eth4.1.

```
Switch#show dot1x interface eth4.1 session-statistics

eth4.1
  SessionOctetsRX: 0
  SessionOctetsTX: 0
  SessionFramesRX: 0
  SessionFramesTX: 0
  SessionId:
  SessionAuthenticationMethod:
  SessionTime: 0
  SessionTerminateCause: PortAdminDisabled
  SessionUserName:

Total Entries: 1
```

show dot1x vlan

Use this command to show the vlan assigned by dot1x module.

show dot1x vlan

Syntax None

Default None

Command Mode EXEC mode or any configuration mode

Usage Guideline None

Example This example shows the output of this command.

```
Switch#show dot1x vlan

   Port    VID
-----------------
eth3.17   100
eth3.18   101

Total Entries: 2
Switch#
```

show dot1x user

Use this command to show the local accounts for 802.1x authentication.

show dot1x user

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline None

Example This example shows the output of this command.

```
Switch#show dot1x user

   Username                                  Password
-------------------------------------------------------------
   yourname1                                 yourpass1
   yourname2                                 yourpass2

Total Entries: 2
```

show errdisable recovery

Use this command to display the error-disable recovery timer related setting.

show errdisable recovery

Syntax None.

Default None

Command Mode EXEC mode or any configuration mode.

Usage Guideline You can use this command to verify the setting of error disable recovery timer.

Example This example shows how to display the setting of error disable recovery timer.

```
Switch# show errdisable recovery
ErrDisable Reason     Timer Status      Timer Interval
------------------    --------------    ----------------
loopback-detection    enable            200 seconds

Interfaces that will be recovered at the next timeout:

Interface    Errdisable Reason    Time left(sec)
---------    -----------------    --------------
eth2.4      loopback-detection   179

Total Entries: 1
```

show enable password

Use this command to display the password of the privilege enable function

show enable password [privilege *LEVEL***]**

Syntax Description	
privilege *LEVEL*	(Optional) Specifies the privilege level.

Default None

Command Mode Privileged EXEC at privilege level 15 or any configuration mode at privilege level 15

Usage Guideline Issuimg this command will display the password of the privilege enable function for either or both privilege level 12 or 15.

Example This example shows how to display all of the enable passwords.

```
Switch# show enable password
Password Encryption : Disabled

Access Level       Password
-------------------------------------------------------------------
12                 mypassword                              (Plain Text)
15                 *@&cRDtpNCeBiq15KOQsKVyrA0sAiCIZQwq      (Encrypted)

Total Entries: 2
Switch#
```

show environment

Use the **show environment** command to display fan, temperature, redundant power system (RPS) availability, and power information for the switch.

show environment [fan | power | temperature]

Syntax Description	
fan	(Optional) Display the detail and status of the switch fans .
power	(Optional) Display the detail and status of the switch power.
temperature	(Optional) Display the detail and status of the switch temperature.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline If a specific environment type is not specified, then all types of environment information will be displayed.

Example The example shows how to display the H/W environmental information.This example includes the thermal sensor status, the operation temperature range, fan operation speed, fan status, and power status.

```
Switch#show environment

Environmental Status

Slot Inlet temperature      Center temperature      Outlet temperature
     current/operation range current/operation range current/operation range
---- ---------------------- ---------------------- ----------------------
1    35 C/0 ~75 C           35 C/0 ~75 C           N/A
2    42 C/0 ~70 C           38 C/0 ~80 C           38 C/0 ~80 C
3    37 C/0 ~76 C           36 C/0 ~77 C           43 C/0 ~75 C
4    42 C/0 ~76 C           36 C/0 ~77 C           38 C/0 ~75 C

Status code: * temperature is out of operation range

Fans are operation in normal speed

Failed Fans: None


Power module     #1             #2             #3             #4
---------------  -------------  -------------  -------------  -------------
Power status     in-operation   empty          empty          empty
Max power        850         W  -              -              -
Used power       203         W  -              -              -


Switch#show environment power

Environmental Status
Power module     #1             #2             #3             #4
---------------  -------------  -------------  -------------  -------------
Power status     in-operation   empty          empty          empty
Max power        850         W  -              -              -
Used power       203         W  -              -              -


Switch#
```

The table below describes the significant fields shown in the display for the power module

Field	Description
Max power	The configured maximum power for the unit.
Used power	The allocated power for the unit
Power status	**In-operation**: The power rectifier is in normal operation mode. **failed:** The power rectifier can't work normally. **empty:** The power rectifier is not installed.

show gvrp configuration

Use the **show gvrp** command to display the settings for gvrp.

show gvrp configuration [interface *INTERFACE-ID* **[, | -]]**

Syntax Description	
interface	Display the gvrp settings of the interface
INTERFACE-ID	(Optional) Specifies the interface to display.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range.
-	(Optional) Specifies a range of interfaces.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline It only displays GVRP related configuration information.

Example This example shows how to display gvrp configuration.

```
Switch# show gvrp configuration

Global GVRP State      : Enabled

Dynamic Vlan Creation : Disabled
Switch#
```

This example shows how to display the GVRP configuration for port's eth3.5 to eth3.6.

```
Switch# show gvrp configuration interface eth3.5-6

Port          GVRP Status    Join    Leave    Leave-All (1/100 Secs)
-----------------------------------------------------------------
eth3.5      Enabled        20      60       1000

eth3.6      Enabled        20      60       1000

Total Entries: 2

Port based Forbidden VLAN Configuration:

Port          Forbidden VLANs
-----------------------------------------------------------------
eth3.5      3,5
eth3.6      5-8

Port based Advertising VLAN Configuration:

Port          Advertising VLANs:

-----------------------------------------------------------------

eth3.5      1,3

eth3.6      1,9

Switch#
```

show gvrp statistics

Use the **show gvrp** statistics command to display the statistics for gvrp ports.

show gvrp statistics [interface *INTERFACE-ID* **[, | -]]**

Syntax Description	
INTERFACE-ID	(Optional) Specifies the interface to display. If no interface is specified, the statistics on all interfaces will be shown.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range.
-	(Optional) Specifies a range of interfaces.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline It only displays the ports which have the gvrp state enabled.

Example This example shows how to display statistics for a range of gvrp ports.

```
Switch# show gvrp statistics interface eth3.5-3.6
Port                JoinEmpty       JoinIn  LeaveEmpty     LeaveIn       Empty
-------------------------------------------------------------------------------
eth3.5     RX               0            0           0           0           0
           TX      4294967296   4294967296  4294967296  4294967296  4294967296
eth3.6     RX               0            0           0           0           0
           TX               0            0           0           0           0

Total Entries: 2
```

show history

To list the commands that have been entered in the current EXEC session, use the **show history** command.

show history

Syntax None

Command Mode User EXEC or any configuration mode

Usage Guideline The switch saves a record of the commands that the user entered. The recorded commands can be recalled to the screen prompt by pressing the following key. CTRL+P or Up Arrow key . They will both recall the commands in a backward sequence. CTRL+N or Down Arrow key will recall the commands in a forward sequence.

The history buffer size is fixed at 20 commands.

Example This example shows how to show the command history.

```
Switch#show history
1 help
2 history
Switch#
```

show interface

Use this command to display information about a specified interface or all interfaces.

show interface [*INTERFACE-ID* **[- | ,]]**

Syntax Description	
INTERFACE-ID	The interface can be a physical port, port-channel and VLAN.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline If no interface is specified, the system will display all existing interfaces.

Examples This example shows sample information output for interface port eth4.1.

```
Switch#show interface eth4.1

eth4.1 is up, line protocol is up (connected)
  Hardware is Ethernet, address is 00-01-02-03-04-00 (bia 00-01-02-03-04-00)
  Description:
  Full-duplex, 100Mb/s, medium type is Fiber, GBIC type is 100BASE-FX
(admin) Send flow-control is off, receive flow-control is off
(oper)  Send flow-control is off, receive flow-control is off
max-rcv-frame-size:1536bytes
  MTU:1500bytes
      RX rate: 9599876 bytes/sec, TX rate: 2399537 bytes/sec
      RX Bytes: 146264046, TX Bytes: 44013446
      RX rate: 141597 packets/sec, TX rate: 37650 packets/sec
      RX Frames: 2102120, TX Frames: 660755
      RX Unicast: 1025389, RX Multicast: 1992
      RX Broadcast: 1074738
      64: 2679551, 65-127: 63295, 128-255: 311
      256-511: 1765, 512-1023: 16388, 1024-1518: 1565
      RX CRC Error: 1, RX Undersize: 0
      RX Oversize: 0, RX Fragment: 0
      RX Jabber: 0, RX Dropped Pkts: 0
      RX MTU Exceeded: 0
      TX CRC Error: 0, TX Excessive Deferral: 0
      TX Single Collision: 0, TX Excessive Collision: 0
      TX Late Collision: 0, TX Collision: 0
Switch#
```

This example is a sample output of information for interface port channel 1.

```
Switch#show interface port-channel1

port-channel1 is down, line protocol is down (notconnect)
  Hardware is Ethernet, address is 00-00-00-00-00-00 (bia 00-00-00-00-00-00)
  Description:
  Members in this channel: 2
        Member   0 : eth4.3   down
        Member   1 : eth4.4   down
```

This example shows sample information output for interface VLAN 1

```
Switch#show interface vlan1

vlan1 is up, line protocol is up (connected)
  Hardware is VLAN, address is 08-01-02-38-00-01 (bia 08-01-02-38-00-01)
  Description:
  IP MTU:1500bytes
```

show interface status err-disabled

Use this command to display a list of interfaces in an error-disabled state, use the **show interfaces status errdisable** command.

show interface status err-disabled

Syntax Description None

Default None

Command Mode EXEC mode or any configuration mode.

Usage Guideline You can use this command to verify which interfaces has been disabled because of an error condition.

Example This example shows how to display the information about the error-disable recovery timer.

```
Switch# show interface status err-disabled
Interface    Status                Reason
---------    ------------------    --------------
eth2.8       err-disabled          loopback-detection
eth4.17      err-disabled          loopback-detection
eth3.10      err-disabled          loopback-detection
```

show ip as-path access-list

To display configured as-path access-lists, use the **show ip as-path access-list** command.

show ip as-path access-list [*ACCESS-LIST-NAME***]**

Syntax Description	
ACCESS-LIST-NAME	(Optional) Specifies the access list to be displayed.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline This command can be used without any arguments. If no arguments are specified, this command will display all as-path access-lists. However, the **as-path** *ACCESS-LIST-NAME* can be specified when entering the **show ip as-path access-list** command. This optionn is 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
AS path access list A1
   permit .*
AS path access list A2
   permit .*
```

show ip bgp

To display entries in the Border Gateway Protocol (BGP) routing table, use the **show ip bgp** command in user EXEC or privileged EXEC mode.

show ip bgp [*IP-ADDRESS***[***/MASK-LENGTH* **[longer-prefixes]] | route-map** *NAME* **]**

Syntax Description	
IP-ADDRESS	(Optional) An IP address entered to filter the output to display only a particular host or network in the BGP routing table.
/MASK-LENGTH	(Optional) Mask length to filter or match hosts that are part of the specified network. It can be in decimal format (i.e. 8).
longer-prefixes	(Optional) Displays the specified route and all other specific routes.
route-map *NAME*	(Optional) Filters the output based on the specified route map.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline The **show ip bgp** command is used to display the contents of the BGP routing table.

Examples The following example output shows the BGP routing table:

```
Switch> show ip bgp
BGP table version: 13, local router ID: 10.1.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop      Metric   LocPrf  Weight   Path
*> 10.1.1.0/24      0.0.0.0            0             32768  i
*> 172.17.1.0/24    192.168.1.1        0                 0  45000 i

Total Entries: 2 entries, 2 routes
Switch>
```

The following is example output from the **show ip bgp** command entered with the **route-map** keyword:

```
Switch(config)#show ip bgp route-map RMAS1
BGP table version is 845, local router ID is 11.0.9.254
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 201.0.1.0/24     11.0.9.1                 0             0 1701 i
*  201.0.2.0/24     11.0.9.1                 0             0 1701 i
*>                   11.0.9.2                 0             0 101 i
*> 201.0.3.0/24     11.0.9.1                 0             0 1701 i
*> 201.0.4.0/24     11.0.9.1                 0             0 1701 i

Total Entries: 4 entries, 5 routes
Switch(config)#
```

The following is example output from the **show ip bgp** command entered with the *IP-ADDRESS* argument:

```
Switch(config)#show ip bgp 121.0.2.0/24
BGP routing table entry for 121.0.2.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to peer-groups:
  G1
  101
    10.50.71.200 from 10.50.71.200 (10.50.71.200)
      Origin IGP, localpref 100, valid, external, best
      Last update: 19:47:01, 2010-09-29
Switch(config)#
```

show ip bgp community-list

To display configured community lists, use the **show ip community-list** command .

show ip bgp community-list *COMMUNITY-LIST-NAME* **[exact-match]**

Syntax Description	
COMMUNITY-LIST-NAME	The configured name of the Community list.
exact-match	(Optional) Displays only routes that have an exact match.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline This command requires the *COMMUNITY-LIST-NAME* to be specified when issued. 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 MarketingCoommunity
BGP table version is 716977, local router ID is 192.168.32.1
Status codes: s suppressed, * valid, > best, i - internal
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric  LocPrf  Weight Path
* i10.3.0.0         10.0.22.1              0    100       0    1800 1239 ?
*>i                 10.0.16.1              0    100       0    1800 1239 ?
* i10.6.0.0         10.0.22.1              0    100       0    1800 690 568 ?
*>i                 10.0.16.1              0    100       0    1800 690 568 ?
* i10.7.0.0         10.0.22.1              0    100       0    1800 701 35 ?
*>i                 10.0.16.1              0    100       0    1800 701 35 ?
*                   10.92.72.24                              0    1878 704 701 35 ?
* i10.8.0.0         10.0.22.1              0    100       0    1800 690 560 ?
*>i                 10.0.16.1              0    100       0    1800 690 560 ?
*                   10.92.72.24                              0    1878 704 701 560 ?
* i10.13.0.0        10.0.22.1              0    100       0    1800 690 200 ?
*>i                 10.0.16.1              0    100       0    1800 690 200 ?
*                   10.92.72.24                              0    1878 704 701 200 ?
* i10.15.0.0        10.0.22.1              0    100       0    1800 174 ?
*>i                 10.0.16.1              0    100       0    1800 174 ?
* i10.16.0.0        10.0.22.1              0    100       0    1800 701 i
*>i                 10.0.16.1              0    100       0    1800 701 i
*                   10.92.72.24                              0    1878 704 701 i

Total Entries: 7 entries, 18 routes
```

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s-The table entry is suppressed. S- The table entry is stale. *-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 entry. The origin code is placed at the end of each line in the table. 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 address of a network entity.
Next Hop	IP address of the next system 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 through autonomous system filters.
Path	Autonomous system paths to the destination network. There can be only one entry in this field for each autonomous system in the path.

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 that match the access list are displayed.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline None

Example This example shows how to display the content of access-list, as-ACL_HQ.

```
Switch> show ip bgp filter-list as-ACL_HQ
BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric  LocPrf  Weight Path
*  172.16.0.0       172.16.72.30           0     109     108    ?
*  172.16.1.0       172.16.72.30           0     109     108    ?
*  172.16.11.0      172.16.72.30           0     109     108    ?
*  172.16.14.0      172.16.72.30           0     109     108    ?
*  172.16.15.0      172.16.72.30           0     109     108    ?
*  172.16.16.0      172.16.72.30           0     109     108    ?
*  172.16.17.0      172.16.72.30           0     109     108    ?
*  172.16.18.0      172.16.72.30           0     109     108    ?
*  172.16.19.0      172.16.72.30           0     109     108    ?
*  172.16.24.0      172.16.72.30           0     109     108    ?
*  172.16.29.0      172.16.72.30           0     109     108    ?
*  172.16.30.0      172.16.72.30           0     109     108    ?
*  172.16.33.0      172.16.72.30           0     109     108    ?
*  172.16.35.0      172.16.72.30           0     109     108    ?
*  172.16.36.0      172.16.72.30           0     109     108    ?
*  172.16.37.0      172.16.72.30           0     109     108    ?
*  172.16.38.0      172.16.72.30           0     109     108    ?
*  172.16.39.0      172.16.72.30           0     109     108    ?

Total Entries: 18 entries, 18 routes
```

show ip bgp neighbors

Use this command to display information about the TCP and Border Gateway Protocol (BGP) connections to neighbors.

show ip bgp [ipv4 { unicast }] neighbors [*IP-ADDRESS* **[advertised-routes | routes]]**

Syntax Description	
ipv4	(Optional) Specifies the address family. The type of address family determines the routing table that is displayed.
unicast	Specifies a IPv4 unicast address family. This is the default option.
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.
routes	(Optional) Displays all accepted routes learned from neighbors.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use the **show ip bgp neighbors** command to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attributes, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

When BGP neighbors use multiple levels of peer templates, it can be difficult to determine which policies are applied to the neighbor.

The output of this command displays all address family information if the keyword **ipv4** is not specified. Specify the IP address of a neighbor to display information about the specific neighbor.

Examples The example on the next page shows how to display the 10.108.50.2 neighbor. This neighbor is an internal BGP (iBGP) peer. This neighbor supports the route refresh and graceful restart capabilities.

```
Switch# show ip bgp neighbors 10.50.71.253
BGP neighbor is 10.50.71.253, remote AS 8001, local AS 8001, internal link
 Member of peer-group G1 for session parameters
  BGP version 4, remote router ID 51.50.71.253
  BGP state = Established, up for 0DT0H39M28S
  Last read 0DT0H39M28S, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    4-Byte AS number: advertised and received
    AS TRANS:
    Address family IPv4 Unicast: advertised and received
  Received 0 in queue
  Sent 0 in queue

                         Sent         Received
  Opens:                 1            0
  Notifications:         1            0
  Updates:               2            2
  Keepalives:            47           45
  Route Refresh:         0            0
  Dynamic Capability:    0            0
  Total:                 51           47
  Connect retry time is 120 seconds
  In update elapsed time is 2367 seconds
  Minimum time between advertisement runs is 5 seconds
  Minimum time between as origination runs is 15 seconds
  Default weight 300

 For address family: IPv4 Unicast
  BGP table version 41, neighbor version 41
  Index 4, Offset 0, Mask 0x10
  G1 peer-group member
  AF-dependant capabilities:
    Graceful restart: advertised, received

  2 accepted prefixes
  3 announced prefixes

 Connections established 1; dropped 0
```

```
 Graceful-restart Status:
  Remote restart-time is 120 sec

Local host: 10.50.71.254, Local port: 179
Foreign host: 10.50.71.253, Foreign port: 49952
Nexthop: 10.50.71.254
Last Reset: 0DT0H39M28S, due to BGP Notification sent
Notification Error Message: (Cease/Unspecified Error Subcode.)
Switch>
```

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 table version: 27, local router ID: 172.16.232.181

Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network       Next Hop           Metric    LocPrf Weight  Path
*>i10.0.0.0      172.16.232.179          0    100          0      ?
*> 10.20.2.0     10.0.0.0                0            32768      i

Total Entries: 2 entries, 2 routes

Swtich>
```

show ip community-list

To display configured community lists, use the **show ip community-lis**t command.

show ip community-list [*COMMUNITY-LIST-NAME***]**

Syntax Description	
COMMUNITY-LIST-NAME	(Optional) Community list name. The community list name can be standard or expanded.

Default None

Command Mode User EXEC or any configuration 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 This example shows how to display the content of all community lists.

```
Switch(config)#show ip community-list
Named Community standard list C1
  permit internet
Named Community standard list C2
  permit 3:2
Switch(config)#
```

show ip dhcp binding

To display the current status of address bindings on the DHCP Server.

show ip dhcp binding [pool *NAME***] [***ADDRESS***]**

Syntax Description	
ADDRESS	(Optional) Specifies the IP address of the DHCP client for which the bindings will be displayed. If no IP address is specified, all bound IP addresses are applied for this command.
pool *NAME*	(Optional) Specifies the pool name for the conflict IP address. If no pool name is specified, all of the pools are applied for this command.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline If the address is not specified, all address bindings are shown. Otherwise, only the binding for the specified client is displayed. The IP address, hardware address, Lease expiration and assigned type will be included in the displayed format.

Examples The following example shows the binding status of all bound IP addresses.

```
switch# show ip dhcp binding
Pool Name: pool1
IP address      Hardware address    Lease start              Lease expiration
----------      ----------------    --------------------   --------------------
10.1.1.1        00b8.3493.32b5      18:38:56, 2010-09-30    18:38:56, 2010-10-1

Pool Name: pool2
IP address      Hardware address    Lease start              Lease expiration
----------      ----------------    --------------------   --------------------
10.1.1.1        00b8.3493.32b5      18:38:56, 2010-09-30    18:38:56, 2010-10-1
10.1.9.1        00b8.3493.32b5      18:38:56, 2010-09-30    18:38:56, 2010-10-1
10.1.11.10      00b8.3493.32b5      18:38:56, 2010-09-30    18:38:56, 2010-10-1
Switch#
```

The following example shows the binding status of the entire address pool2,

```
switch# show ip dhcp binding pool pool2
IP address      Hardware address    Lease start              Lease expiration
----------      ----------------    --------------------   --------------------
10.1.1.1        00b8.3493.32b5      18:38:56, 2010-09-30    18:38:56, 2010-10-1
10.1.9.1        00b8.3493.32b5      18:38:56, 2010-09-30    18:38:56, 2010-10-1
10.1.11.10      00b8.3493.32b5      18:38:56, 2010-09-30    18:38:56, 2010-10-1
```

The following example shows the binding status of IP address 10.1.1.1 in DHCP address pool, pool1.

```
switch# show ip dhcp binding pool pool1 10.1.1.1
IP address     Hardware address    Lease start              Lease expiration
----------     ----------------    --------------------   --------------------
10.1.1.1       00b8.3493.32b5      18:38:56, 2010-09-30   18:38:56, 2010-10-1
```

show ip dhcp conflict

To display the conflict IP addresses while a DHCP Server attempts to assign the IP addresses for a client.

show ip dhcp conflict [pool *NAME*]**[***ADDRESS*]

Syntax Description	
ADDRESS	(Optional) Specifies the conflict IP address. If no conflict IP address is specified, all conflict IP addresses are applied.
pool *NAME*	(Optional) Specifies the pool name for the conflict IP address. If no pool name is specified, all pools are applied for this command.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline The DHCP server detects the conflict by the ping operation. If a conflict address is found, then the IP address found will be removed from address pool and marked as conflict and will not be assigned until a network administrator clears this conflict. If the address is not specified, all conflict addresses are shown. Otherwise, only the conflict address for the specified address is displayed. The IP address, Detection Method and Detection Time will be included in the displayed format. If a duplicate IP address is detected by the DHCP server, the Detection Method will be marked as "ping" and if the duplicate IP address is detected by the DHCP client, the Detection Method will be marked as "Gratuitous ARP".

Example The following example shows the conflict status of IP address 10.1.1.1.

```
switch# show ip dhcp conflict 10.1.1.1
Pool name: pool2
IP address      Detected Method    Detection time
----------      ---------------    --------------
10.1.1.1        Ping                 18:38:56, 2010-09-30
```

The following example shows the conflict status of all DHCP IP address pools.

```
switch# show ip dhcp conflict
Pool name: pool2
IP address      Detected Method    Detection time
----------      ---------------    --------------
10.1.1.1        Ping                 18:38:56, 2010-09-30

Pool name: pool3
IP address      Detected Method    Detection time
----------      ---------------    --------------
172.1.1.1        Gratuitous ARP    18:38:56, 2010-09-30
```

show ip dhcp pool

To display information about the Dynamic Host Configuration Protocol (DHCP) address pools,

show ip dhcp pool [*NAME***]**

Syntax Description	
NAME	(Optional) Displays information about a specific address pool. If not specified, displays information about all address pools.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use this command to examine the current utilization level and configuration setting of the address pool. If the *NAME* argument is not used then the information for all the pools will be displayed.

Example The following example shows DHCP address pool information for an On-Demand Address Pool (ODAP), pool 1. The table below describes the significant fields in the display.

```
switch# show ip dhcp pool2
Pool name: pool2
  Accept client ID: Yes
  Accept relay Agent: No
  Boot file: boot.bin
  Default router: 10.1.2.1
  DNS server: 10.1.2.1
  Domain name: alphanetworks.com
  Lease: 3600 seconds
  NetBIOS node type: hybrid
  NetBIOS scpoe ID: alpha
  Next server: 10.1.2.1
  Subnet:255.255.0.0
  Based-on mac-address:00:01:02:03:04:05-00:01:02:03:04:FF
  Based-on mac-address:00:08:02:03:04:05
  Based-on mac-address:00:09:02:03:04:05
  Based-on client ID: 0x01000102030405
  Based-on C-VID: 2
  Based-on C-VID: 10-20
  Based-on S-VID: 100
  Based-on S-VID: 300-400
  Based-on interface ip-address: 10.0.3.1
  Based-on relay-ip-address: 10.5.3.1
  Based-on vendor-class: Alpha
  Based-on user-class: MSFT

IP addresses: total 511
10.0.0.1
10.0.1.1-10.0.1.255
10.0.3.1-10.0.3.255
Number of leased address: 100
Number of conflict addresses: 2
switch#
```

Display Field Descriptions Descriptions of the significant fields in the previous example.

Field	Description
Pool	The name of the pool.

Field	Description
Subnet	The bit combination with the address of the DHCP address pool
Lease	The duration of the lease for an IP address
Accept client ID	To validate the DHCP Client Identifier value sent by the client or not
Accept relay agent	Accept DHCP packet contains option82 or not. This control can be one of the following configurations: Remote-ID & Circuit-ID, Remote ID Circuit-ID No.
Domain name	The domain name for DHCP clientBoot fileThe name of the default boot image for a Dynamic Host Configuration Protocol (DHCP) client
Next server	The configured IP addresses of next-server
Default router	The default router list for a DHCP client
DNS server	The IP address list of DNS server available to DHCP clients.
NetBIOS node type	the NetBIOS node type
NetBIOS scpoe ID	the NetBIOS scope id
WINS server	The IP address of WINS server
Based-on mac-address	The address binding rule based on MAC
Based-on client ID	The address binding rule based on Client ID
Based-on C-VID	The address binding rule based on customer vlan id
Based-on S-VID	The address binding rule based on service provider vlan id
Based-on interface-ip-address	The address binding rule based on ingress interface IP
Based-on relay-ip-address	The address binding rule based on IP address of relay agent
Based-on vendor-class	The address binding rule based on vendor class (option60)
Based-on user-class	The address binding rule based on user class (option77)
Number of leased address	The number of addresses has been leased .
Number of conflict addresses	The number of addresses are conflict with other clients.

show ip dhcp relay

Display the IP DHCP relay agent configuration.

show ip dhcp relay

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Display the DHCP relay agent configuration

Example This example shows how to display the DHCP relay agent configuration.

```
Switch# show ip dhcp relay
DHCP Relay                          : Enabled
Relay Hop Count                     : 4
DHCP Relay Information Option       : Enabled
DHCP Relay Information Policy       : keep
DHCP Relay Information Check Reply  : Enabled
DHCP Relay Information Trusted      : Enabled
VLAN100 Relay IP Addresses
10.1.1.1, 10.1.1.2 , 10.1.1.3 , 0.0.0.0
List of Trusted sources of relay agent information option:
VLAN100             VLAN200             VLAN300             VLAN400
Switch#
```

show ip dhcp relay information trusted-sources

Use the s**how ip dhcp relay information trusted-sources** command to display all interfaces configured to be a trusted source for the Dynamic Host Configuration Protocol (DHCP) relay information option, .

show ip dhcp relay information trusted-sources

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Display the DHCP relay agent configuration.

Example The following is sample output when the **ip dhcp relay information trusted** command is configured. Note that the display output lists the interfaces that are configured to be trusted sources.

```
Switch# show ip dhcp relay information trusted-sources
List of trusted sources of relay agent information option:
VLAN100    VLAN200    VLAN300    VLAN400    VLAN500
Total Entries: 5
Switch#
```

show ip dhcp server

This command displays the current status of DHCP server

show ip dhcp server

Syntax None

Default None

Command Mode Privileged EXEC

Usage Guideline Display the DHCP server status and user configured pool.

Example This example shows how to display the status of DHCP server.

```
Switch# show ip dhcp server
DHCP server: Disable
Ping packets number: 3
Ping timeout: 500 ms

List of DHCP server configured address pool

pool1               pool2               pool3               pool4
pool5               pool6               pool7               pool8
pool9               pool10              pool11              pool12
```

show ip dhcp server statistics

To display Dynamic Host Configuration Protocol (DHCP) server statistics.

show ip dhcp server statistics

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline The **show ip dhcp server statistics** command displays the DHCP counters. All counters are cumulative.

Example The following example resets all DHCP counters to zero. The table below describes the significant fields in the display.

```
switch# show ip dhcp server statistics
Address pools      2
Malformed messages 0
Renew  messages    0

Message            Received
BOOTREQUEST        12
DHCPDISCOVER       200
DHCPREQUEST        178
DHCPDECLINE        0
DHCPRELEASE        0
DHCPINFORM         0

Message            Sent
BOOTREPLY          12
DHCPOFFER          190
DHCPACK            172
DHCPNAK            6
switch#
```

Display Field Descriptions Significant field descriptions for command **show ip dhcp server statistics**

Field	Description
Address pools	The number of configured address pools in the DHCP database.
Malformed messages	The number of truncated or corrupted messages that were received by the DHCP server.

Field	Description
Renew messages	The number of renew messages for a DHCP lease. The counter is incremented when a new renew message has arrived after the first renew message.
Message	The DHCP message type that was received by the DHCP server.
Received	The number of DHCP messages that were received by the DHCP server.
Sent	The number of DHCP messages that were sent by the DHCP server.

show ip dhcp snooping

Use this command to display DHCP snooping configuration.

show ip dhcp snooping

Syntax Description Not applicable.

Default Not applicable.

Command Mode EXEC mode or any configuration mode.

Usage Guideline Use the command to display DHCP snooping configuration setting.

Example This example shows how to display DHCP Snooping configuration:

```
Switch# show ip dhcp snooping
DHCP Snooping is enabled.
DHCP Snooping is enabled on VLANs:
Vlan10, vlan15-18
Information option: not allowed
Interface    Trusted    Rate Limit
---------- ---------- --------------
eth3.1         no         10
eth3.8         no         50
eth3.9         yes


Switch#
```

show ip dvmrp interface

This command is used to display dvrmp configuration information on interface.

show ip dvmrp interface [*INTERFACE-ID* **[,|-]]**

Syntax Description	
INTERFACE-ID **[** , | - **]**	(Optional) Specifies a single interface, a range of interfaces separated by a hyphen, or a series of interfaces separated by a comma. If no interface is specified, the switch displays DVRMP information on all interfaces at which DVMRP is enabled (That is for all of DVMRP enabled interfaces). Only VLAN interface are allowed to be specified for this command.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline This command displays interface related information about Distance Vector Multicast Routing Protocol (DVMRP).

Example This example shows how to display the DVMRP configuration information about interface VLAN 1000.

```
Switch#show ip dvmrp interface vlan1000
Interface  Address          Metric  Generation ID
---------  ---------------  ------  -------------
vlan1000   10.0.0.254       1       1234567890

Total Entries: 1
Switch#
```

show ip dvmrp neighbor

Use this command to show DVMRP neighbor information.

show ip dvmrp neighbor [*INTERFACE-ID* **|** *IP-ADDRESS* **] [detail]**

Syntax Description	
INTERFACE-ID	(Optional) Specifies the interface ID
IP-ADDRESS	(Optional) The IP address of the neighbor
detail	(Optional) Show the neighbor information in detail.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use this command to display DVMRP neighbor information. If neither *INTERFACE-ID* nor *IP-ADDRESS* is specified, then the information of all neighbors will be displayed. If the keyword of **detail** is not specified, then only brief information for the neighbors will be displayed.

Examples This example shows how to display neighbor information.

```
Switch>show ip dvmrp neighbor
Interface        Neighbor Address  Generation ID  ExpTime
---------------  ----------------  -------------  -----------
vlan1            10.10.10.11       0035ef6d       0DT0H0M29S

Total Entries: 1
```

Display Field Descriptions Description of the significant display fields.

Display Field	Description
Interface	The interface refers to the routing interface which is mapped to a VLAN interface.
Neighbor Address	Once a system has received a Probe from a neighbor that contains the system's address in the neighbor list, then the system has established a two-way neighbor adjacency with this router.
Generation ID	If a DVMRP router is restarted, it will not be aware of any previous prunes that it had sent or received. In order for the neighbor to detect that the router has restarted, a non-decreasing number is placed in the periodic probe message called the generation ID. When a change in the generation ID is detected, any prune information received from the router is no longer valid and should be flushed.

ExpTime	The *neighbor time-out interval,* which SHOULD be set to 35 seconds. This setting allows early detection of a lost neighbor yet provides tolerance for busy multicast routers. These time-out values MUST be coordinated between all DVMRP routers of a particular physical network segment. The expire time shown here is the amount of time remaining before reaching the *neighbor time-out interval* setting.

This example shows how to display neighbor detail information.

```
Switch>show ip dvmrp neighbor detail
Capability Flags: N-Network, S-SNMP,M-MTRACE, G-GENID, P-PRUNE, L-LEAF
Neighbor address: 10.10.10.11
Interface: vlan1
UpTime:         0DT0H23M49S
ExpTime:        0DT0H0M30S
Generation ID: 0035ef6d
Major Version: 3
Minor Version: 255
Capabilities:  e  (Flags: M,G,P)
Number of bad routes Received:      0
Number of routes Received:          0
Number of PROBE Received:           144
Number of REPORT Received:          1
Number of PRUNE Received:           0
Number of GRAFT Received:           0
Number of GRAFTACK Recvd:           0
```

Display Field Descriptions Description of the significant display fields.

Display Field	Description
Capability Flags	LEAF - Whether this neighbor router is a leaf router. PRUNE - This neighbor router understands pruning. GENID- This neighbor router sends Generation Id's. MTRACE - This neighbor router handles Mtrace requests. SNMP - This neighbor router supports the DVMRP MIB. Network - This neighbor will accept a network mask.

UpTime	The total time elapsed since the neighbor was discoved until now.
ExpTime	The time remaining until the entry is removed from the DVMRP neighbor table.
Generation ID	If a DVMRP router is restarted, it will not be aware of any previous prunes that it had sent or received. In order for the neighbor to detect that the router has restarted, a non-decreasing number is placed in the periodic probe message called the generation ID. When a change in the generation ID is detected, any prune information received from the router is no longer valid and should be flushed.

show ip dvmrp prune

Use this command to display DVMRP upstream prune state information.

show ip dvmrp prune

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Display DVMRP upstream Prune state information.

Example This example shows how to displays prune information.

```
DGS-6600:15#show ip dvmrp prune
Flags: P=Pruned,D=Holddown,N=NegMFC

Source              Group             State ExpTime      Prune/Graft
Network             Address                              ReTransmit-Time
------------------ ---------------- ----- ------------ --------------
10.0.7.101/32       239.255.255.250  P..   0DT1H45M44S  Off
10.0.7.131/32       239.255.255.250  P..   0DT1H47M30S  Off
10.1.52.99/32       229.55.150.208   P.N   0DT1H44M36S  0DT0H3M50S

Total Entries: 3
```

Display Field Descriptions Description of significant display fields.

Display Field	Description
Source Network	The address of the source IP address or source network.
Group Address	The IP group address.
State	P: The upstream state is in Prune state. D: The entry is in Hold-Down state. In this state, a negative multicast forwarding cache (ip mroute) entry will be added. N: Negative Multicast forwarding cache (ip mroute) is installed.
ExpTime	The amount of time remaining before this prune will expire.
Prune/Graft ReTransmit Time	The ramaining time before retransmitting a Prune or Graft. When "P" flag is set in the "State" field, this timer would represent the Prune retransmit timer, otherwise, it would represent the Graft retransmit timer.

show ip dvmrp route

Use this command to display DVMRP route information.

show ip dvmrp route [*NETWORK-ADDRESS* **]**

Syntax Description	
NETWORK-ADDRESS	(Optional) Specifies the source network address and mask length be displayed. If NETWORK-ADDRESS is not specified, all DVMRP routes will be displayed.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Display DVMRP route information.

Example This example shows how to display route information.

```
DGS-6600:15#show ip dvmrp route
State: H = Hold-down
Source Network     Upstream Neighbor Metric Learned Interface State ExpTime
------------------ ----------------- ------ ------- --------- ----- ------------
10.0.0.0/8         10.78.62.51       1      Local   vlan99          -

Total Entries: 1
DGS-6600:15#
```

Display Field Descriptions Description of significant display fields.

Display Field	Description
Source Network	The address of the source IP address or source network.
Upstream neighbor	The Next hop router to the source network. 0.0.0.0: This route is a local interface entry, and therefore it does not enable DVMRP. If the interface is a local entry, then the upstream neighbor displays its own interface IP address.
Learned	Indicates this route entry is a local interface. The other condition is dynamically learned.
Interface	The local Interface used to connect to the source network.
State	Route state displays "H" if the DVMRP route is in "Hold-down" state.
ExpTime	The time remaining until the entry is removed from the DVMRP routing table. A dash note indicates this entry is not going to be removed (because it is a local interface).

show ip igmp group

Used to display IGMP group information on an interface

show ip igmp group [*IP-ADDRESS* **| interface** *INTERFACE-ID***] [detail]**

Syntax Description	
IP-ADDRESS	(Optional) Specifies the Group IP address to display. If no IP address is specified, all IGMP group information will be displayed.
interface *INTERFACE-ID*	(Optional) Specifies the interface to display. If no interface is specified, IGMP group information of all interfaces where IGMP is enabled will be displayed.
detail	(Optional) Specifies to show the additional information (Uptime, Expires, Group mode and Last reporter).

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline User can display IGMP group information by using this command. The following examples cover different versions of IGMP. The uptime means the time elapsed since the entry is created. The expire time means the time that the entry will be removed if there is no refresh of the entry,

Examples This example shows how to display IGMP group information for interface VLAN 1000.

```
Switch#show ip igmp group interface vlan1000
Interface        Group Address   Uptime     Expires      Last Reporter
-----------------------------------------------------------------------
vlan1000          224.0.1.149    0DT0H0M9S  0DT0H4M15S   10.10.0.91

Total Entries : 1 entries, 2 records
Switch#
```

Display Field Descriptions show ip igmp group Field Descriptions.

Field	Description
entries	The number of the igmp group table display.
records	The number of the group records and source records in the igmp group table.

This example shows how to display IGMP group detailed information for group 224.1.1.1. If the interface is operated at v3, the group source list will be displayed. If the interface is not operated at v3, the group source list will not be displayed.

```
Switch# show ip igmp group 224.1.1.1 detail
Interface      : vlan1000
Group          : 224.1.1.1
Uptime         : 0DT0H0M42S
Expires        : stopped
Group mode     : Include, dynamic
Last reporter  : 192.168.50.111

Group source list:
       Source Address    Uptime      v3 Exp       Forward
     ------------------------------------------------------
       192.168.55.55     0DT0H0M42S  0DT0H3M38S     Yes
       192.168.10.55     0DT0H0M10S  0DT0H3M38S     Yes

Interface     : vlan2000
Group         : 224.1.1.1
Uptime        : 0DT0H0M42S
Expires       : 0DT0H3M38S
Group mode    : Exclude, dynamic
Last reporter : 192.168.51.111
Source list is empty
```

Display Field Descriptions Description of significant display fields.

Display Field	Description
Uptime	The time elapsed since the entry has been created in the format of [n]DT[n]H[n]M[n]S.
Expires	The time that the entry will be removed if there is no refresh on the entry in the format of [n]DT[n]H[n]M[n]S. **stopped** indicates that timing out of this entry is not determined by this expire timer. If the router is in Include mode for a group, then the whole group entry times out after the last source entry has timed out (unless the mode is changed to Exclude mode before it times out).
Group mode	Include or Exclude: The group mode is based on the type of membership reports that are received on the interface for the group. **dynamic**: If this port (or port-channel) interface receives a host's IGMP membership report for the group.
Last reporter	Last host to report being a member of the multicast group.
Forward	Status of whether the router is forwarding multicast traffic due to this entry.

show ip igmp interface

Used to display IGMP configuration information on interface

show ip igmp interface [*INTERFACE-ID* **[, | -]]**

Syntax Description	
INTERFACE-ID **[**,|-**]**	(Optional) Specifies a single interface, a range of interfaces separated by a hyphen, or a series of interface separated by a comma. If no interface is specified, the switch displays IGMP information for all interfaces where IGMP is enabled (that is for all of IGMP enabled interfaces). Note, only a VLAN interface type is allowed for this command.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline User can display Interface IGMP configuration information by this command.

If the specified VLAN interface has IGMP disabled, all of the IGMP related configuration shown as if IGMP is enabled with the exception that the IGMP state is disabled. When no VLAN interface is specified, only IGMP enabled VLANs are displayed for this command. While a VLAN interface list may incorporate IGMP disabled VLANs, all of the listed VLAN's IGMP configuration information is displayed.

Example This example shows how to display IGMP configure information about interface VLAN 1000.

```
Switch#show ip igmp interface vlan1000
vlan1000
  IP Address/Netmask               : 10.50.95.90/8
  IGMP State                       : Enabled
  Access Group                     : igmp_fileter
  Version                          : 3
  Query Interval                   : 125 seconds
  Query Maximum Response Time      : 10 seconds
  Robustness Value                 : 2
  Last Member Query Interval       : 1000 milliseconds
  Querier                          : 10.50.95.90
  Querier Timer countdown value     : -
  Configured Query Interval         : 5
  Configured Maximum response time  : 15
  Configured Robustness             : 2
```

show ip igmp snooping

Use this command to display IGMP Snooping information on the switch.

show ip igmp snooping [VLAN *VLAN-ID***]**

Syntax Description	
VLAN *VLAN-ID*	(Optional) Specifies a VLAN. The VLAN ID range is 1 to 4094. If no VLAN is specified, then this command shows IGMP Snooping Information for all VLANs where IGMP Snooping is enabled (i.e. all IGMP Snooping enabled VLAN interfaces).

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline The IGMP Snooping information can be displayed using this command. If the specified VLAN does not exist or IGMP Snooping is disabled at the VLAN, an error message will be displayed.

Example This example shows how to display IGMP Snooping configurations.

```
Switch> show ip igmp snooping
IGMP Snooping is enabled in the following VLANs
Codes- v3:IGMP v3 host compatibility mode, v2: IGMP v2 host compatibility mode
v1:IGMP v1 host compatibility mode
   Vlan  Querier state      Querier Router      Immediate      Timer State
                                                Leave
   -----  -------------     ---------------     ---------      ------------
(v3)1    Enabled            Active              Enabled        -
(v2)2    Disabled           -                   Disabled       0DT0H4M10S
(v3)3    Enabled            Non-active          Enabled        0DT0H3M12S
Total number of VLANs = 3
Switch>
```

Display Field Descriptions The following table shows the field information for the above example.

Display Field	Parameter	Description
Querier state	Enabled	IGMP Snooping querier is enabled.
	Disabled	IGMP Snooping querier is disabled.
Querier Router	Active	This VLAN interface of the switch works as an IGMP snooping querier.
	Non-active	This VLAN interface does not function as an IGMP snooping querier.
	-	This field can be disregarded when the IGMP snooping querier state is disabled.
Immediate Leave	Enable	IGMP Snooping immediate leave response function is enabled which means the member port of the VLAN interface will receive any IGMP leave message from a port, the system will immediately remove the port from the multicast group membership.
	Disable	IGMP Snooping immediate leave response function is disabled which means the member port of the VLAN interface will receive the IGMP leave message, the system will not remove the port from the multicast group membership, instead the system will follow IGMP interaction process to confirm the multicast membership.
Host Compatibility Mode	IGMPv1 IGMPv2 IGMPv3	The current compatibility state of this interface. This state is dependent on the version of general queries received from the interface. IGMPv3 is the default value. If any lower version is received, the version will go back to the lowest version for backward compatibility.
Timer State	-	The timer stops counting down.
	[n]DT[n]H[n]M[n]S	Timer starts to count down, and its initial count is set to the value got from the Older Version Querier Present Timeout in the IGMP control packet.

show ip igmp snooping group

Use this command to display IGMP Snooping group information learned by the switch.

show ip igmp snooping group [*IP-ADDRESS* **| VLAN** *VLAN-ID* **] [detail]**

Syntax Description	
IP-ADDRESS	(Optional) Specifies the Group IP address to display. If no IP address is specified, all IGMP Snooping group information will be displayed.
VLAN *VLAN-ID*	(Optional) Specifies the VLAN interface to display. If no VLAN is specified, the command shows IGMP snooping group information about all VLANs where IGMP Snooping is enabled.
detail	(Optional) Specifies to show the additional information (Uptime, Expires, Group mode and Last reporter).

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline User can display IGMP Snooping group information by this command. The following examples cover different versions of the IGMP.

If the specified VLAN does not exist or IGMP Snooping is disabled at the VLAN, an error message will be displayed instead.

Examples This example shows how to display IGMP Snooping group information.

```
Switch# show ip igmp snooping group
IGMP Snooping Connected Group Membership: ((s)- static configuration)
Group address  Source address   Interface    Port
-------------  --------------- --------     ---------
224.0.1.149      10.2.2.18       vlan1       eth3.12
224.0.1.145      10.1.1.2        vlan1       eth3.15
224.0.2.123(s)   10.3.3.128      vlan2       eth3.1

Total Entries : 3 entries, 6 records
```

Display Field Descriptions show ip igmp snooping group Field Descriptions.

Field	Description
entries	The number of the igmp snooping group table display.
records	The number of the group records and source records in the igmp snooping group table.

This example shows how to display the IGMP snooping group detailed information of group 224.1.1.1. If the interface is operated at v3, the group source list will be displayed. If the interface is not operated at v3, the group source list will not be displayed.

```
Switch# show ip igmp snooping group 224.1.1.1 detail
IGMP version: V3
Interface: vlan1000
Group: 224.1.1.1
Port: eth3.12
Uptime       : 0DT0H0M42S
Expires      : stopped
Group mode   : Include, dynamic
Last reporter: 192.168.50.111

Source Address     Uptime        v3 Exp       Forward
---------------  ------------  ------------  ---------
192.168.55.55     0DT0H0M42S     0DT0H3M38S    yes
192.168.55.66     0DT0H0M42S     0DT0H3M38S    no

IGMP version: V2
Interface    : vlan2000
Group        : 224.1.1.1
Port         : eth3.2
Uptime       : 0DT0H0M42S
Expires      : 0DT0H3M38S
Group mode   : Exclude, dynamic
Last reporter: 192.168.51.111
Source list is empty
Switch#
```

Display Field Descriptions The following table shows the display field information for the example on the previous page.

Display Field	Description
IGMP version	The version of IGMP. The version of IGMP that the multicast group has reported.
Interface	Interface ID of VLAN in which the multicast IP address is reported.
Uptime	The time elapsed since the entry has been created in the format of [n]DT[n]H[n]M[n]S
Expires	The time that the entry will be removed if there is no refresh on the entry in the format of [n]DT[n]H[n]M[n]S. "**never**" indicates that the entry will not be time out, because a local receiver is on the router for this entry. "**stopped**" indicates that the time-out of this entry is not determined by this expire timer. If the router is set to *Include mode* for a group, then the whole group entry times out after the last source entry has timed out (unless the mode is changed to *Exclude mode* before it times out).
Group mode	Include or Exclude: The group mode is based on the type of membership reports that are received on the interface for the group. **static**: If this group is configured statically on the port (or port-channel) interface. **dynamic**: If this port (or port-channel) interface receives a host's IGMP membership report for the group.
Last reporter	Last host to report being a member of the multicast group.
Forward	Status of whether the router is forwarding multicast traffic due to this entry.

show ip igmp snooping mrouter

Use this command to display IGMP Snooping mrouter information learned and configured on the switch.

show ip igmp snooping mrouter [vlan *VLAN-ID***] [designate | auto | not-allowed]**

Syntax Description	
vlan *VLAN-ID*	(Optional) Specifies a VLAN. The VLAN ID range is 1 to 4094. If no VLAN is specified, this command shows IGMP snooping information on all VLANs where IGMP snooping is enabled.
designate	(Optional) Display the router ports which are statically configured.
auto	(Optional) Display the router ports which are dynamically learned.
not-allowed	(Optional) Display the router ports which are configured as forbidden to be router ports.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline This command is used to display information on dynamically learned and manually configured multicast router interfaces. When IGMP snooping is enabled, the switch automatically learns the interface to which a multicast router is connected. These are dynamically learned interfaces. If no option is specified, all of designate, auto, and not-allowed interfaces are displayed.

When the specified VLAN does not exist or the specified VLAN is without IGMP snooping enabled, a warning message will appear indicating this.

Example This example shows how to display IGMP snooping mrouter information.

```
Switch# show ip igmp snooping mrouter
vlan1
Designate   : eth3.4,
Auto        : eth4.2,
Not-allowed: -
vlan2
Designate   : eth4.4,
Auto        : eth3.2,
Not-allowed: -
Total Entries: 2
```

show ip interface

Use this command to display the information of ip interfaces.

show ip interface [*INTERFAC E-ID* **] [brief]**

Syntax Description	
INTERFACE-ID	(Optional) Interface type and number. It refers to an IP interface, that is VLAN interfaces only.
brief	(Optional) Displays a summary of the usability status information for each interface.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline An IP interface can be in either the down state or up state. When an interface is in the up state, it can send and receive packets. If an interface is in the down state, the directly connected routing entry is removed from the routing table. Removing the entry allows the switch to use dynamic routing protocols to determine backup routes to the network.

If an optional interface type is specified, then information for that specific interface is displayed. This command only supports VLAN interface types.

If no optional arguments are specified, then information for all the interfaces is displayed.

If the interface hardware is usable, the interface is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.

Example This example shows how to display the brief format of the **show ip interface** command.

```
Switch> show ip interface brief
Interface              IP-Address     Status           Protocol
-------------------------------------------------------------
vlan1                10.90.90.90      up                 up
vlan2                20.1.1.1         up                 up

Total Entires: 2

Switch>
```

This example shows how to display the ip interface information for VLAN 1

```
Switch> show ip interface vlan1
  vlan1 is up,
  Internet address is 100.0.0.1/24
  Internet address is 110.0.0.1/24  (secondary)
  MAC Address is 08-01-02-24-00-01
  ARP timeout is 14400 seconds
  IP MTU is 1500 bytes
```

show ip key-chain

Use this command to display the settings of the configured key chains.

show ip key-chain *[NAME-OF-KEY]*

Syntax Description	
NAME-OF-KEY	(Optional) Specifies the name of a key chain to display.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Specify the name of key-chain (N*AME-OF-KEY*) to get the information of specific key-chain. If no NAME-OF-KEY is specified, information of all key-chains will be shown.

Example The following example shows the sample output of show ip key-chain:

```
Switch# show ip key-chain
Key-Chain tree
  Key 1 -- text "stringforkey1"
    accept lifetime (13:30:00 Jan 25 2008) - (15:29:59 Jan 25 2008)
    send lifetime (14:30:00 Jan 25 2008) - (16:29:59 Jan 25 2008)
  Key 2 -- text "stringforkey2"
    accept lifetime (14:30:00 Jan 25 2008) - (always valid)
    Send-lifetime 14:30:00 Jan 25 2008 duration 3600
Key-Chain ifall
  Key 1 -- text "admin123"
    accept lifetime (13:30:00 Feb 25 2008) - (15:29:59 Feb 25 2008)
    send lifetime (14:30:00 Feb 25 2008) - (16:29:59 Feb 25 2008)
  Key 2 -- text "guestabc"
    accept lifetime (13:30:00 Feb 25 2008) - (15:29:59 Feb 25 2008)
    send lifetime (14:30:00 Feb 25 2008) - (16:29:59 Feb 25 2008)
Switch#
```

show ip mroute

Use this command to display the content of the IP multicast routing table.

show ip mroute [{ [group-addr *GROUP-ADDRESS* **] [source-addr** *NETWORK-ADDRESS* **] [summary] } |static]**

Syntax Description	
group-addr *GROUP-ADDRESS*	(Optional) Specifies the Group IP address.
source-addr *NETWORK-ADDRESS*	(Optional) Specifies the Source IP network address.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.
static	(Optional) Displays the multicast static routes

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Displays the content of the IP multicast table.

The “Uptime” timer describes the time elapsed since the entry was created.

The “Expires” timer is a keep-alive timer for the multicast data stream. The Expires timer value is based on either the PIM Sparse and Dense Mode RFCs (RFC 4601 and RFC 3973) or DVMRP. If the multicast data continues to arrive at the device, the timer will renew itself.

If network address is specified, the switch displays the entries with source addresses that match the specified address.

Example This example shows how to display the IP multicast route table summary:

```
Switch> show ip mroute summary
IP Multicast Routing Table: 1 entry
Flags: D - PIM-DM, S - PIM-SM, V - DVMRP
Timers: Uptime/Expires


(10.10.1.52, 224.0.1.3), vlan1, 0DT0H1M32S/0DT0H3M20S, Flags: D
```

The following is sample output from the **show ip mroute** command.

```
Switch> show ip mroute
IP Multicast Routing Table - 1 entry
Flags: D - PIM-DM, S - PIM-SM, V - DVMRP
Timers: Uptime/Expires


 (10.10.1.52, 224.0.1.3), uptime 0DT5H29M15S, expires 0DT0H2M59S, flags: D
Incoming interface: vlan1
Outgoing interface list:
vlan2
vlan3
```

The following is a sample output from the **show ip mroute static** command.

```
Switch> show ip mroute static
Mroute: 192.168.6.0/24, RPF neighbor: 10.1.1.1, distance: 0
Mroute: 192.168.7.0/24, RPF neighbor: 10.1.1.1, distance: 100
Mroute: 192.168.8.0/24, interface: Null, distance: 0

Total Entries: 3
```

show ip ospf

Use this command to display general information about the OSPF routing process.

show ip ospf

Syntax None

Default None

Command Mode User EXEC

Usage Guideline Display general OSPF protocol information. It provides system-wide statistics and per area statistics for OSPF. The LSDB database overflow limit is the capacity for the LSA table size. It is project dependent.

Example On the following page is a sample output from the **show ip ospf** command.

```
Switch#show ip ospf
 Operational Router ID 10.47.65.160
 Process uptime is 0DT0H12M33S
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 This router is an ABR, ABR Type is Standard (RFC2328)
 This router is an ASBR (injecting external routing information)
 This router is a BR
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Number of external LSA 1240. Checksum 0x26DB197
 Number of router LSA 17
 Number of network LSA 10
 Number of non-default summary LSA 109
 Number of asbr summary LSA 38
 Number of non-default external LSA 1240
 Number of LSA originated 138
 Number of LSA received 1441
 Number of current LSA 1426
 LSDB database overflow limit is 24576
 Number of areas attached to this router: 5
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 5 active interface number is 5
        Number of fully adjacent neighbors in this area is 5
        SPF algorithm last executed 0DT0H9M46S ago
        SPF algorithm executed 9 times
        Number of LSA 66
        Network 47.65.49.0/24
        Summarize  range 3.0.0.0/8  advertise  cost 1 (auto)
    Area 0.0.0.1
        Number of interfaces in this area is 2 active interface number is 2
        Number of fully adjacent neighbors in this area is 2
        Number of fully adjacent virtual neighbors through this area is 2
        SPF algorithm last executed 0DT0H9M46S ago
        SPF algorithm executed 7 times
        Number of LSA 32
        Network 47.65.51.0/29
        Network 47.65.52.0/29

Switch#
```

show ip ospf border-routers

Use this command to display the ABRs and ASBRs for the OSPF instance.

show ip ospf border-routers

Syntax None

Default None

Command Mode User EXEC

Usage Guideline Use this command to display the ABRs and ASBRs information.

Example This is a sample output from the **show ip ospf border-routers** command

```
Switch#show ip ospf border-routers

OSPF process internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 10.47.65.181 [1] via 47.65.51.2, vlan51, ABR, ASBR, TransitArea 0.0.0.1
i 10.47.65.182 [1] via 47.65.52.2, vlan52, ABR, ASBR, TransitArea 0.0.0.1
i 10.47.65.183 [1] via 47.65.53.2, vlan53, ABR, ASBR, TransitArea 0.0.0.2
i 10.47.65.184 [1] via 47.65.54.2, vlan54, ABR, ASBR, TransitArea 0.0.0.2
i 47.65.131.111 [2] via 47.65.52.2, vlan52, ASBR, TransitArea 0.0.0.1
i 47.65.151.111 [2] via 47.65.53.2, vlan53, ASBR, TransitArea 0.0.0.2
Total Entries: 6

Switch#
```

show ip ospf database

Use this command to display a database summary for OSPF information.

show ip ospf database

Syntax None

Default None

Command Mode User EXEC

Usage Guideline Display information about the database summary for OSPF information.

Example The following page shows a sample output from the **show ip ospf database** command:

```
Switch#show ip ospf database

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.47.65.160    10.47.65.160    1765 0x8000000e 0x107f 6


                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
47.65.49.111    47.65.49.111    1819 0x80000001 0x33da


                Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Route
2.1.1.0         10.47.65.160      57 0x80000002 0xe15a 2.1.1.0/24


                ASBR-Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.47.65.160    10.47.65.181    1786 0x80000003 0xb756


                Router Link States (Area 0.0.0.61 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.47.65.160    10.47.65.160      77 0x80000004 0x24bb 1

                Summary Link States (Area 0.0.0.61 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum  Route
2.1.1.0         10.47.65.160      57 0x80000002 0xff3e 2.1.1.0/24


                NSSA-external Link States (Area 0.0.0.61 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum  Route              Tag
1.0.0.0         10.47.65.160     117 0x80000002 0x80e7 N2 1.0.0.0/24      0


                AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route              Tag
1.0.0.0         10.47.65.160     107 0x80000002 0x15e5 E2 1.0.0.0/24      0

Total Entries: 8

Switch#
```

show ip ospf database asbr-summary

Use this command to display information about the Autonomous System Boundary Router (ASBR) summary LSAs.

show ip ospf database asbr-summary[*LINK-STATE-ID***|self-originate|adv-router** *IP-ADDRESS***]**

Syntax Description	
LINK-STATE-ID	Link State ID (as an IP address).
self-originate	Self-originated link states.
adv-router	Displays all the LSAs of the specified router.
IP-ADDRESS	Advertise router IP address.

Default None

Command Mode User EXEC

Usage Guideline Displays information about the Autonomous System Boundary Router (ASBR) summary LSAs.

Example The following page shows a sample output from the **show ip ospf database asbr-summary** command.

```
Switch#show ip ospf database asbr-summary

                ASBR-Summary Link States (Area 0.0.0.0)

  LS age: 893
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: ASBR-summary-LSA
  Link State ID: 10.47.65.160 (AS Boundary Router address)
  Advertising Router: 10.47.65.181
  LS Seq Number: 80000003
  Checksum: 0xb756
  Length: 28
  Network Mask: /0
        TOS: 0  Metric: 1


                ASBR-Summary Link States (Area 0.0.0.1)

  LS age: 927
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: ASBR-summary-LSA
  Link State ID: 10.47.65.183 (AS Boundary Router address)
  Advertising Router: 10.47.65.160
  LS Seq Number: 80000001
  Checksum: 0x53ba
  Length: 28
  Network Mask: /0
        TOS: 0  Metric: 1

Total Entries: 2

Switch#
```

show ip ospf database external

Use this command to display information about the external LSAs.

show ip ospf database external [*LINK-STATE-ID*|**self-originate|adv-router** *IP-ADDRESS* **]**

Syntax Description	
LINK-STATE-ID	Link State ID (as an IP address).
self-originate	Self-originated link states.
adv-router	Displays all the LSAs of the specified router.
IP-ADDRESS	Advertise router IP address.

Default None

Command Mode User EXEC

Usage Guideline Display information about the Autonomous System Boundary Router (ASBR) external LSAs.

Example The below is a sample output from the **show ip ospf database externa**l command.

```
Switch#show ip ospf database external

                AS External Link States

  LS age: 1056
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 1.0.0.0 (External Network Number)
  Advertising Router: 10.47.65.160
  LS Seq Number: 80000001
  Checksum: 0x17e4
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        Forward Address: 47.65.52.2
        External Route Tag: 0

Total Entries: 1

Switch#
```

show ip ospf database network

Use this command to display information about the network LSAs.

show ip ospf database external [*LINK-STATE-ID***|self-originate|adv-router** *IP-ADDRESS***]**

Syntax Description	
LINK-STATE-ID	Link State ID (as an IP address).
self-originate	Self-originated link states.
adv-router	Displays all the LSAs of the specified router.
IP-ADDRESS	Advertise router IP address.

Default None

Command Mode User EXEC

Usage Guideline Display information about the network LSAs.

Example This is a sample output (on the next page) from the **show ip ospf database network** command

```
Switch#show ip ospf database network

                Net Link States (Area 0.0.0.0)

  LS age: 1034
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: network-LSA
  Link State ID: 47.65.49.111 (address of Designated Router)
  Advertising Router: 47.65.49.111
  LS Seq Number: 80000001
  Checksum: 0x33da
  Length: 32
  Network Mask: /24
        Attached Router: 47.65.49.111
        Attached Router: 10.47.65.160


                Net Link States (Area 0.0.0.1)

  LS age: 1015
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: network-LSA
  Link State ID: 47.65.51.2 (address of Designated Router)
  Advertising Router: 10.47.65.181
  LS Seq Number: 80000001
  Checksum: 0x9ea1
  Length: 32
  Network Mask: /29
        Attached Router: 10.47.65.181
        Attached Router: 10.47.65.160

Total Entries: 2

Switch#
```

show ip ospf database nssa-external

Use this command to display information about the nssa-external LSAs.

how ip ospf database nssa-external [*LINK-STATE-ID***| self-originate|adv-router** *IP-ADDRESS***]**

Syntax Description	
LINK-STATE-ID	Link State ID (as an IP address).
self-originate	Self-originated link states.
adv-router	Displays all the LSAs of the specified router.
IP-ADDRESS	Advertise router IP address.

Default None

Command Mode User EXEC

Usage Guideline Display information about the nssa-external LSAs.

Example This is a sample output (on the next page) from the **show ip ospf database nssa-external** command.

```
Switch#show ip ospf database nssa-external

                NSSA-external Link States (Area 0.0.0.61 [NSSA])

  LS age: 1161
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 1.0.0.0 (External Network Number For NSSA)
  Advertising Router: 10.47.65.160
  LS Seq Number: 80000001
  Checksum: 0x82e6
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        NSSA: Forward Address: 110.201.0.1
        External Route Tag: 0

  LS age: 1097
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 47.65.55.0 (External Network Number For NSSA)
  Advertising Router: 10.47.65.160
  LS Seq Number: 80000001
  Checksum: 0xbb07
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        NSSA: Forward Address: 110.201.0.1
        External Route Tag: 0

 Total Entries: 2

Switch#
```

show ip ospf database router

Use this command to display information about the router LSAs.

show ip ospf database router [*LINK-STATE-ID*|**self-originate|adv-router** *IP-ADDRESS* **]**

Syntax Description	
LINK-STATE-ID	Link State ID (as an IP address).
self-originate	Self-originated link states.
adv-router	Displays all the LSAs of the specified router.
IP-ADDRESS	Advertise router IP address.

Default None

Command Mode User EXEC

Usage Guideline Display information about the router LSAs.

Example The following pages shows a sample output from the **show ip ospf database router** command.

```
Switch#show ip ospf database router

                Router Link States (Area 0.0.0.0)

  LS age: 1056
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x3 : ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.47.65.160
  Advertising Router: 10.47.65.160
  LS Seq Number: 8000000e
  Checksum: 0x107f
  Length: 96
   Number of Links: 6

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 47.65.49.111
     (Link Data) Router Interface address: 47.65.49.1
      Number of TOS metrics: 0
       TOS 0 Metric: 1

    Link connected to: a Virtual Link
     (Link ID) Neighboring Router ID: 10.47.65.181
     (Link Data) Router Interface address: 47.65.51.1
      Number of TOS metrics: 0
       TOS 0 Metric: 1

    Link connected to: a Virtual Link
     (Link ID) Neighboring Router ID: 10.47.65.182
     (Link Data) Router Interface address: 47.65.52.1
      Number of TOS metrics: 0
       TOS 0 Metric: 1

    Link connected to: a Virtual Link
     (Link ID) Neighboring Router ID: 10.47.65.183
     (Link Data) Router Interface address: 47.65.53.1
      Number of TOS metrics: 0
       TOS 0 Metric: 1
```

```
    Link connected to: a Virtual Link
      (Link ID) Neighboring Router ID: 10.47.65.184
      (Link Data) Router Interface address: 47.65.54.1
       Number of TOS metrics: 0
        TOS 0 Metric:

    Link connected to: Stub Network
      (Link ID) Network/subnet number: 47.65.49.112
      (Link Data) Network Mask: 255.255.255.255
       Number of TOS metrics: 0
        TOS 0 Metric: 0

  LS age: 1063
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x3 : ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.47.65.181
  Advertising Router: 10.47.65.181
  LS Seq Number: 80000006
  Checksum: 0xb55d
  Length: 48
   Number of Links: 2

    Link connected to: a Virtual Link
      (Link ID) Neighboring Router ID: 10.47.65.160
      (Link Data) Router Interface address: 47.65.51.2
       Number of TOS metrics: 0
        TOS 0 Metric: 1

    Link connected to: a Virtual Link
      (Link ID) Neighboring Router ID: 10.47.65.184
      (Link Data) Router Interface address: 47.65.84.2
       Number of TOS metrics: 0
        TOS 0 Metric: 10

 Total Entries: 2

Switch#
```

show ip ospf database summary

Use this command to display information about the summary LSAs.

how ip ospf database summary [*LINK-STATE-ID***|self-originate|adv-router** *IP-ADDRESS* **]**

Syntax Description	
LINK-STATE-ID	Link State ID (as an IP address).
self-originate	Self-originated link states.
adv-router	Displays all the LSAs of the specified router.
IP-ADDRESS	Advertise router IP address.

Default None

Command Mode User EXEC

Usage Guideline Display information about the summary LSAs.

Example The following page shows a sample output from the **show ip ospf database summary** command.

```
Switch#show ip ospf database summary

                Summary Link States (Area 0.0.0.0)

  LS age: 1225
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: summary-LSA
  Link State ID: 2.1.1.0 (summary Network Number)
  Advertising Router: 10.47.65.160
  LS Seq Number: 80000001
  Checksum: 0xe359
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 1

  LS age: 1225
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: summary-LSA
  Link State ID: 2.1.2.0 (summary Network Number)
  Advertising Router: 10.47.65.160
  LS Seq Number: 80000001
  Checksum: 0xd863
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 1

 Total Entries: 2

Switch#
```

show ip ospf host-route

Use this command to display host-route information for OSPF.

show ip ospf host-route

Syntax None.

Default None

Command Mode User EXEC

Usage Guideline Use this command to display host route information for OSPF.

Example The following is a sample output of this command:

```
Switch# show ip ospf host-route

Host IP          AreaID               Cost

-----------------------------------------------

10.3.3.3         0.0.0.5              2
10.3.3.4         0.0.0.1              3
20.3.3.3         0.0.0.25             58

Total Entries: 3
```

show ip ospf interface

Use this command to display interface information for OSPF.

show ip ospf interface [*IFNAME* **]**

Syntax Description	
IFNAME	(Optional) Specifies the interface type of the interfaces to display the OSPF information for.

Default None

Command Mode User EXEC

Usage Guideline Use this command to display interface information for OSPF. If no IFNAME is specified the OSPF information for all interfaces will be displayed.

Example The following example on the next page is a sample output of this command:

```
Switch#show ip ospf interface
 vlan49 is up, line protocol is up
  Internet Address 47.65.49.1/24, Area 0.0.0.0, MTU 1500
  Router ID 10.47.65.160, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1000 sec, State BDR, Priority 1
  Designated Router (ID) 47.65.49.111, Interface Address 47.65.49.111
  Backup Designated Router (ID) 10.47.65.160, Interface Address 47.65.49.1
  Timer intervals configured, Hello 20, Dead 80, Retransmit 10
  Hello due in 0DT0H0M9S
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 39 sent 39, DD received 25 sent 14
  LS-Req received 0 sent 1, LS-Upd received 2 sent 947
  LS-Ack received 588 sent 3, Discarded 0
  Current Authentication Type: none
 vlan51 is up, line protocol is up
  Internet Address 47.65.51.1/29, Area 0.0.0.1, MTU 1500
  Router ID 10.47.65.160, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 2
  Designated Router (ID) 10.47.65.181, Interface Address 47.65.51.2
  Backup Designated Router (ID) 10.47.65.160, Interface Address 47.65.51.1
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Hello due in 0DT0H0M5S
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 68 sent 69, DD received 26 sent 22
  LS-Req received 0 sent 0, LS-Upd received 11 sent 9
  LS-Ack received 5 sent 11, Discarded 0
  Current Authentication Type: md5
  Authentication  Key Configuration
    Authentication type: md5
      message-digest-key 254 md5 80008001
Switch#
```

show ip ospf neighbor

Use this command to display information about the OSPF neighbors.

show ip ospf neighbor [*IFNAME* **|** *NEIGHBOR-ID***] [detail]**

Syntax Description	
IFNAME	(Optional) Specifies the type of the interface to display the neighbor information for.
NEIGHBOR-ID	(Optional) Neighbor ID.
detail	(Optional) Detail of neighbors.

Default None

Command Mode User EXEC

Usage Guideline Displays information about the OSPF neighbors. If no interface type/number is specified the OSPF neighbor information for all interfaces will be displayed.

Example The following is sample output from the **show ip ospf neighbor**.

```
Switch#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time      Address
Interface
47.65.49.111      2   Full/DR         0DT0H1M11S     47.65.49.111    vlan49
Total Entries: 1
Switch#
Switch#
Switch#show ip ospf neighbor detail
 Neighbor 47.65.49.111, interface address 47.65.49.111
    In the area 0.0.0.0 via interface vlan49
    Neighbor priority is 2, State is Full, 6 state changes
    DR is 47.65.49.111, BDR is 47.65.49.1
    Options is 0x02 (*|-|-|-|-|-|E|-)
    Dead timer due in 0DT0H1M13S
    Neighbor is up for 0DT0H13M51S
    Crypt Sequence Number is 0

Total Entries: 1
Switch#
```

show ip ospf virtual-links

Use this command to display virtual link information.

show ip ospf virtual-links

Syntax None

Default None

Command Mode User EXEC

Usage Guideline Use this command to display virtual link information.

Example The following pages show sample outputs from the **show ip ospf neighbor**.

```
Switch#show ip ospf virtual-links
Virtual Link   to router 10.47.65.181 is up
  Transit area 0.0.0.1 via interface vlan51
  Local address 47.65.51.1/32
  Remote address 47.65.51.2/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
    Hello due in 0DT0H0M9S
    Adjacency state Full
  Current Authentication Type: none
Virtual Link   to router 10.47.65.182 is up
  Transit area 0.0.0.1 via interface vlan52
  Local address 47.65.52.1/32
  Remote address 47.65.52.2/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
    Hello due in 0DT0H0M3S
    Adjacency state Full
  Current Authentication Type: simple text
  Authentication  Key Configuration
    Authentication type: simple text
      Authentication-key: 12345678
Virtual Link   to router 10.47.65.183 is up
  Transit area 0.0.0.2 via interface vlan53
  Local address 47.65.53.1/32
  Remote address 47.65.53.2/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
    Hello due in 0DT0H0M10S
    Adjacency state Full
  Current Authentication Type: none
Virtual Link   to router 10.47.65.184 is up
  Transit area 0.0.0.2 via interface vlan54
  Local address 47.65.54.1/32
  Remote address 47.65.54.2/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
    Hello due in 0DT0H0M5S
    Adjacency state Full
  Current Authentication Type: md5
  Authentication  Key Configuration
    Authentication type: md5
      message-digest-key 255 md5 1234567890123456
```

show ip pim

Use this command to show the PIM global information.

show ip pim

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use this command to display the global information of PIM.

Example The following example displays PIM global information.

```
Switch##show ip pim
PIM Configurations:
Register Checksum Include Data: Disabled, group-list: (None)
Register Suppression Time      : 60 seconds
Accept Register Group list     : pim-acp-reg

RP Address
  90.1.1.1, group-list: static-rp

RP Candidate
  vlan100, group-list: rp-cand, interval: 60, priority: 192

BSR Candidate
  vlan100, hash-mask-length: 30, priority: 1
```

show ip pim bsr

Use this command to show the bootstrap router (BSR) information.

show ip pim bsr

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use this command to display the elected BSR information and information about the locally configured for the candidate rendezvous point (RP) advertisement.

Examples The following example displays the BSR information on a BSR router with the Candidate RP information on the router's interface, vlan100.

```
Switch# show ip pim bsr
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 90.1.1.3
  Uptime:      0DT0H18M50S, BSR Priority: 3, Hash mask length: 30
  Next bootstrap message in 0DT0H0M21S

  Candidate RP: 90.1.1.3(vlan100) Group acl:5
    Next Cand_RP_advertisement in 0DT0H0M13S
```

The following example displays the BSR information on a non-BSR router with Candidate RP information on the router's interface

```
Switch# show ip pim bsr
PIMv2 Bootstrap information
BSR address: 90.1.1.3
Uptime: 0DT0H0M38S, BSR Priority: 3, Hash mask length: 30
Expires: 0DT0H1M32S

Switch#
```

show ip pim interface

Use this command to show the interface information.

show ip pim interface [*INTERFACE-ID***] [detail]**

Syntax Description	
INTERFACE-ID	(Optional) Specifies the interface to display the interface information for. Only VLAN interface IDs are applicable.
detail	(Optional) Use to display the interface information in detail.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use this command to display interface related information. If no interface is specified, the PIM information on all applicable interfaces will be shown.

Examples The following example displays interface information.

```
switch #show ip pim interface
Address         Interface  Mode   Neighbor DR      DR              Generation
                                  Count    Priorty                 ID
--------------- ---------- ------ -------- ------- --------------- ----------
90.1.1.1        vlan100    Sparse 1        1       90.1.1.1        164598300
30.1.1.1        vlan200    Dense  1        0       0.0.0.0         375693

Total Entries: 2
```

On the following page is an example which displays the interface information in detail.

```
switch#show ip pim interface detail

vlan100
  Address                   : 90.1.1.1
  Mode                      : Sparse
  Neighbor Count            : 1
  DR                        : 90.1.1.1
  DR Priotity               : 1
  DR Priority Enabled       : Enabled
  Generation ID             : 164598300
  Hello Interval            : 30 seconds
  Triggered Hello Interval  : 5 seconds
  Hello Hold time           : 105 seconds
  Join Prune Interval       : 60 seconds
  Join Prune Hold Time      : 210 seconds
  Stub Interface            : False
  Lan Delay Enabled         : Enabled
  Propagation Delay         : 1000 milliseconds
  Override Interval         : 3000 milliseconds
  Effect Propag Delay       : 1000 milliseconds
  Effect Override Interval  : 3000 milliseconds
  Join Suppression Enabled  : Enabled
  Bidir Capable             : False

vlan200
  Address                   : 50.111.111.111
  Mode                      : Dense
  Neighbor Count            : 1
  DR                        : 0.0.0.0
  Generation ID             : 375693
  Hello Interval            : 30 seconds
  Triggered Hello Interval  : 5 seconds
  Hello Hold time           : 105 seconds
  Stub Interface            : False
  Lan Delay Enabled         : Enabled
  Propagation Delay         :  500 milliseconds
  Override Interval         : 2500 milliseconds
  Effect Propag Delay       :  500 milliseconds
  Effect Override Interval  : 2500 milliseconds
  Prune Limit Interval      : 60 seconds
  Graft Retry Interval      : 3 seconds
  State Refresh Priority Enabled    : Enabled
  State Refresh Origination Interval: 60 seconds
```

show ip pim mroute

This command displays the PIM IP multicast routing table

show ip pim mroute

Syntax Description None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use this command to display all entries in the IP multicast routing table.

The switch populates the multicast routing table by creating source, group (S,G) entries from star, group (*,G) entries. The star (*) refers to all source addresses, the "S" refers to a single source address, and the "G" is the destination multicast group address. When creating (S,G) entries, the software uses the best path to that destination group which is found in the unicast routing table (that is, through Reverse Path Forwarding [RPF]).

Example The following page shows a sample output from the command **show ip pim mroute**.

```
Switch#show ip pim mroute
PT - Prune Timer, PPT - Prune Pending Timer, ET - Expiry Timer,
PLT - Prune Limit Timer, GRT - Graft Retry Timer,
AT - Assert Timer, KAT - Keep Alive Timer, OT - Override Timer,
SAT - Source Active Timer, SRT - State Refresh Timer

Flags: D - Dense, S - Sparse, T - SPT-bit set

(*,239.1.1.1) Uptime: 0DT0H31M15S,  flags: S
  RP: 70.1.1.3, RPF neighbor:30.1.1.3, RPF Interface: vlan1
  Upstream Interface:
    Join State: Joined, Join Timer: 39 secs
  Downstream Interface List:
    Vlan2:
      JP State: No Info, ET:Off, PPT: Off
      Assert State: No Info, AT: Off,
      Assert Winer: 0.0.0.0, Metric: 0, Pref: 0,


(70.233.235.100, 239.1.1.1) Uptime: 0DT0H3M8S, flags: ST
  RPF neighbor: None, RPF Interface: None
  Register State: Pruned, Register Stop Timer: 20 secs
  Upstream Interface:
    Join State: Joined, Join Timer: off, KAT: 22 secs,
  Downstream Interface List:
    Vlan2
      JP State: No Info , ET: 20 secs, PPT: Off
      Assert State: No Info, AT: Off,
      Assert Winer: 0.0.0.0, Metric: 0, Pref: 0

(70.233.235.100, 239.1.1.1, rpt) Uptime: 0DT0H3M8S, flags: S
  RP: 70.1.1.3, RPF neighbor: None, RPF interface: None
  Upstream Interface:
    Prune State: RPT Not Joined, Override Timer: Off
  Downstream Interface List:
    vlan2
      Prune State: No Info, ET: Off, PPT: Off
(90.233.235.100, 239.1.1.100) Uptime: 0DT0H1M8S, flags: D
  State-Refresh Originator State: Originator
  SAT: 200 secs , SRT: 30 secs
  Upstream Interface:
    vlan100, Prune State: No Info, Assert State: No Info
    GRT: off, OT: off, PLT: off  Downstream Interface List:
    vlan200
      JP State: No Info, PT: Off, PPT: off
      Assert State: No Info, AT: Off,
      Assert Winer: 0.0.0.0, Metric: 0, Pref: 0
```

show ip pim neighbor

Use this command to show the PIM-SM neighbor information.

show ip pim neighbor [*INTERFACE-ID***]**

Syntax Description	
INTERFACE-ID	(Optional) Specifies the interface to display the PIM-SM neighbor information for. If *INTERFACE-ID* is not specified, the information on all interfaces will be displayed.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use this command to determine which routers on the LAN are configured for PIM.

Example The following example displays the PIM neighbor information for all interfaces.

```
Switch# show ip pim neighbor
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      S - State Refresh Capable
Neighbor        Interface Uptime/Expires             Ver   DR Pri/Mode
-------------------------------------------------------------------------
---
10.10.0.9       vlan1     0DT0H55M33S/0DT0H1M44S     v2    1 /
10.10.0.136     vlan1     0DT0H55M20S/0DT0H1M25S     v2    1 /
10.10.0.172     vlan1     0DT0H55M33S/0DT0H1M32S     v2    1 / DR
192.168.0.100   vlan2     0DT0H55M30S/0DT0H1M20S     v2    N

Total Entries: 4
Switch#
```

Display Field Descriptions The following table describes the ip pim neighbor fields.

Field	Descriptions
DR Pri/Mode	Priority and mode of the designated router (DR). Priority: "N" indicates the neighbor does not support DR Priority Option in the Hello message otherwise the DR priority value will be displayed. Mode: Describes the capability of the neighbor. The meaning of codes is as follows:

Field	Descriptions
DR Pri/Mode	B: bidirectional mode, neighbor is using the Bidirectional-PIM Capable option. DR: indicates the neighbor is the Designated Neighbor. If an empty string is displayed it indicates the neighbor is not a DR. S: State Refresh Capable. The neighbor is using the State Refresh Capable option. This option is used only by PIM-DM.

show ip pim rp mapping

Use this command to show group-to-RP (rendezvous point) mappings, and the RP set.

show ip pim rp mapping

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use this command to display active rendezvous points (RPs) that are cached with associated multicast routing entries.

This command is used to display the RP mapping information viewed by the router

Example The following is sample output from the **show ip pim rp mapping** command with the group address 239.1.1.1 specified:

```
Switch#show ip pim  rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
RP: 90.1.1.3
Info source: 90.1.1.3, via bootstrap, priority 0
Uptime: 0DT16H52M39S, expires: 0DT0H2M50S
```

Display Field Descriptions The table below shows the ip pim rp mapping detailed field descriptions.

Field	Descriptions
RP	Address of the RP for the group specified.
Info source	Indicates from which system the router learned this RP information. RP was selected by the bootstrap mechanism. In this case, the BSR is also the RP.
Via bootstrap	The RP mapping information is learned from RP.
Priority	The RP priority
Uptime	Length of time that the router has known about this RP.
Expires	Time after which the information about this RP expires. If the router does not receive any refresh messages in this time, it will discard information about this RP.

show ip pim rp-hash

Use this command to display the rendezvous point (RP) to be chosen based on the group selected.

show ip pim rp-hash *GROUP-ADDRESS*

Syntax Description	
GROUP-ADDRESS	Specifies the Group Address to display the selected RP of the group for.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline This command displays which RP was selected for the group specified. It also shows whether this RP was selected by Auto-RP or the PIM Version 2 bootstrap mechanism.

Example The following is sample output from the **show ip pim rp-hash** command with the group address 239.1.1.1 specified:

```
Switch#show ip pim  rp-hash 239.1.1.1
RP: 172.16.24.12
Info source: 172.16.24.12, via bootstrap
Uptime: 0DT1H42M15S, expires: 0DT0H2M16S
```

Please refer to the table in the description of command **show ip pim rp mapping** for the field descriptions.

show ip protocols

Use this command to display the state of the dynamic routing process.

show ip protocols [rip] [ospf] [bgp]

Syntax Description	
rip	(Optional) RIP protocol information is displayed.
ospf	(Optional) Display OSPF global settings which are related to the overall IP routing function.
bgp	(Optional) Display entries in the Border Gateway Protocol (BGP) routing table. Specifies the autonomous system to be displayed. .

Default If no option is specified, the summary of all running routing protocols is displayed.

Command Mode User EXEC or any configuration mode

Usage Guideline The information displayed by the **show ip protocols** command is useful when debugging routing operations. The output can help identify a router suspected of delivering faulty routing information.

Examples The following example shows how to output the state of the RIP protocol:

```
Switch# show ip protocols rip
Routing Protocol is "rip"
  Sending updates every 30 +/- (0 to 5) seconds, next due in 19 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Default redistribution metric is 1
  Redistributing:
    type            metric
    ------------------------

  Default version control: send version 2, receive version 2
    Interface        Send  Recv  V2-broadcast    Key-chain
    vlan141          2     2     Off
  Routing for Networks:
    vlan141 (10.253.41.2/24)
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
    10.253.41.1           120  0DT0H0M11S               0           1
   the maximum number of RIP routes allowed: 12288
  Number of routes (excluding connected): 3
  Distance: (default is 120)
Switch#
```

The table below describes the **show ip protocols** Field Descriptions for a RIP Process:

Field	Description
Routing Protocol is "rip"	Specifies the routing protocol used.
Sending updates every 30 seconds	Specifies the time between sending updates.
next due in 2 seconds	Precisely when the next update is due to be sent.
Invalid after 180 seconds	Specifies the value of the invalid parameter.
garbage collect after 120	Specifies the time (in seconds) after which the individual routing information will be thrown (flushed) out.
Default version control:	Specifies the version of RIP packets that are sent and received.
Redistributing	Lists the protocol that is being redistributed.
Routing	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the operating system software is using to build its routing table. For each source, the following will be displayed: • IP address • Administrative distance • Time the last update was received from this source

The following example shows how to output the state of OSPF protocol:

```
Switch# show ip protocols ospf
Routing Protocol is "ospf"
 Configured Router ID: 10.253.41.2
 Redistribute route default metric:auto
 Auto-cost Reference-bandwidth:100
 Distance: (default is 110)
 Do not originate type 5 default route
 Redistributing:
  type            metric    mtric_type
  ---------------------------------------
  rip             20        2


Switch#
```

show ip rip database

To display summary address entries in the Routing Information Protocol (RIP) routing database entries, use the **show ip rip database** command.

show ip rip database

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline **show ip rip database** will display route information, such as: network, next hop, metric, from, if, time.

Examples The following output shows a summary address.

```
Switch# Show ip rip database
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
    Network       Next Hop   Metric From          If       Time
Rc 10.0.0.0/8                              1                  vlan1
Rc 20.0.0.0/8                              1                  vlan2
R 30.0.0.0/8  20.33.24.1            2 20.33.24.1  vlan2    0DT0H2M44S
                      40.33.24.8            5 40.33.24.2  vlan3    0DT0H2M30S

Total Entries: 3 entries, 4 routes
Switch#
```

Display Field Descriptions Description of significant display fields.

Display Field	Description
Rc 10.0.0.0/8	Directly connected entry to vlan1.
Rc 20.0.0.0/8	Directly connected entry to vlan2.
R 30.0.0.0/8 via ,etc.	The destination 30.0.0.0/8 is learned via RIP. There are two sources advertising it. One is 20.33.24.1 via vlan2 and it was updated 16 seconds ago. The other source is 40.33.24.8 via vlan3, and it was updated 30 seconds ago.

show ip rip interface

Display interface specific information for RIP.

show ip rip interface [*INTERFACE-ID***]**

Syntax Description	
interface *INTERFACE-ID*	(Optional) Specifies the interface ID to display the RIP information for. If no INTERFACE-ID is specified, the RIP information on all interfaces will be shown.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline **show ip rip interface** will display interface specific information, such as: authentication, send version, receive version, and v2 broadcast mode.

Example The following output shows the **show ip rip interface** command:

```
Switch# Show ip rip interface

vlan1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Send v2-broadcast: Disabled
    Authentication Mode: text
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.72.63.80/8
vlan2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Send v2-broadcast: Disabled
    Authentication Mode: text
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      20.72.63.80/8
```

show ip route

To display the current state of the routing table, use the **show ip route** command.

show ip route [IP-ADDRESS **[***MASK***] | [database] [***PROTOCOL* **| connected | static]]**

Syntax Description	
IP-ADDRESS	(Optional) Address about which routing information should be displayed.
MASK	(Optional) Argument specifying a subnet mask.
PROTOCOL	(Optional) The name of a routing protocol, specifying a routing protocol, use one of the following keywords: bgp, ospf, and rip.
database	(Optional) Specifies that the routing database is to be shown and the active routes populated in the forwarding database is prefixed with an asterisk.
connected	(Optional) Display all connected local interface routes.
static	(Optional) Display all static routes.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline The show ip route database static command displays, for example, all static routes with name and distance information, including active and inactive entries. Display all active static routes with both the **show ip route** and **show ip route static** commands.

Examples The following examples show the standard routing tables displayed by the show ip route command. Use the codes displayed at the beginning of each report and the information in the following table to understand the types of routes.

Field	Description
O	Indicates the protocol that derived the route. It can be one of the following values: **K** - kernel route **R** - Routing Information Protocol (RIP) derived **O** - Open Shortest Path First (OSPF) derived **C** - connected **i** - IS-IS **ia - IS-IS**-inter area * - candidate default **S** - static **B** - Border Gateway Protocol (BGP) derived
E2	Type of route. It can be one of the following values: ***** - Indicates the last path used when a packet was forwarded. It pertains only to the nonfast-switched packets. However, it does not indicate which path will be used next when forwarding a nonfast-switched packet, except when the paths are equal cost. **IA** - OSPF interarea route **E1** - OSPF external type 1 route **E2** - OSPF external type 2 route **L1** - IS-IS Level 1 route **L2** - IS-IS Level 2 route **N1** - OSPF not-so-stubby area (NSSA) external type 1 route **N2** - OSPF NSSA external type 2 route **P** - stale route info
*	The route entry of RIB is populated in FIB.
>	The selected route of multiple route entries.
10.110.0.0	Indicates the address of the remote network.

Field	Description
[160/5]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next router to the remote network.
0DT0H0M44S	Specifies the last time the route was updated.
Vlan2	Specifies the interface through which the specified network can be reached.
Total Entries :	Displays the the total number of entries, and the total number of routes.

The following is sample output from the **show ip route** command when entered without an address:

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default

C        10.0.0.0/8 is directly connected, vlan10
O        10.50.71.253/32 [110/0] is a summary, Null, 0DT1H5M46S
C        11.0.0.0/8 is directly connected, vlan110
O E1     11.0.1.0/24 [110/1] via 11.50.71.200, vlan110, 0DT1H4M47S
C        12.0.0.0/8 is directly connected, vlan111
C        20.0.0.0/8 is directly connected, vlan111
O E1     20.0.1.0/24 [110/1] via 11.50.71.200, vlan110, 0DT1H4M47S
O IA     50.0.0.0/8 [110/2] via 10.50.71.253, vlan10, 0DT1H3M58S
B        121.0.0.0/24 [20/0] via 10.50.71.200, vlan10, 0DT1H5M35S
B        121.0.1.0/24 [20/0] via 10.50.71.200, vlan10, 0DT1H5M35S
B        121.0.2.0/24 [20/0] via 10.50.71.200, vlan10, 0DT1H5M35S
S        160.0.0.0/8 [1/0] via 10.50.71.200, vlan10

Total Entries: 12 entries, 12 routes
```

The following example shows output of the **show ip route database** command.

```
Switch#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       > - selected route, * - FIB route, p - stale info

C    *> 10.0.0.0/8 is directly connected, vlan10
O    *> 10.50.71.253/32 [110/0] is a summary, Null, 0DT1H7M18S
C    *> 11.0.0.0/8 is directly connected, vlan110
O E1 *> 11.0.1.0/24 [110/1] via 11.50.71.200, vlan110, 0DT1H6M19S
C    *> 12.0.0.0/8 is directly connected, vlan111
C    *> 20.0.0.0/8 is directly connected, vlan111
O E1 *> 20.0.1.0/24 [110/1] via 11.50.71.200, vlan110, 0DT1H6M19S
B       50.0.0.0/8 [200/0] via 10.50.71.253, 0DT1H5M21S
O IA *> 50.0.0.0/8 [110/2] via 10.50.71.253, vlan10, 0DT1H5M30S
B    *> 121.0.0.0/24 [20/0] via 10.50.71.200, vlan10, 0DT1H7M7S
B    *> 121.0.1.0/24 [20/0] via 10.50.71.200, vlan10, 0DT1H7M7S
B    *> 121.0.2.0/24 [20/0] via 10.50.71.200, vlan10, 0DT1H7M7S
S    *> 160.0.0.0/8 [1/0] via 10.50.71.200, vlan10

Total Entries: 13 entries, 13 routes
```

show ip route summary

To display the current state of the routing table, use the **show ip route summary** command.

show ip route summary

Syntax Description None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline None

Example The following is sample output from the **show ip route summary** command:

```
Switch#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table multi-paths state is enabled
IP routing table configured maximum-paths is 6
IP routing table maximum-paths is 6
Route Source    Networks
connected       2
rip             1
bgp             2
Total           5
FIB             3
multi-path      0
```

show ip ssh

Use this command to display the user SSH configuration setting.

show ip ssh

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use the show ip ssh command to view the status of configured options such as retries and timeouts. This command displays if SSH is enabled or disabled.

Example This example shows how to display the SSH configuration settings.

```
Switch# show ip ssh
SSH                     : Enabled
SSH server mode         : V2
Service port            : 22
Authentication timeout  : 120
Authentication retries  : 3
Switch#
```

show ip trusted-host

Use this command to display the trusted host information on the device.

show ip trusted-host [snmp | http | https | telnet | ssh]

Syntax Description	
[snmp | http | https | telnet | ssh]	(Optional) Specifies which access interface which is to be displayed. If no access interface is specified, the trusted hosts at all access interfaces will be displayed.

Default None

Command Mode Privileged EXEC or any configuration mode at privilege level 15

Usage Guideline This command displays the trusted host information.

Example This example shows how to display trusted hosts information for all access interfaces.

```
Switch# show ip trusted-host
Hosts                   Valid to Access
-------------------------------------
10.48.93.100            all access interfaces
10.51.17.1              snmp
10.52.95.90             http

Total Entries : 3
Switch#
```

show ipv6 dhcp

This command is used to display DHCPv6 client configuration running information of interface(s).

show ipv6 dhcp [interface [*INTERFACE-NAME* **]]**

Syntax Description	
interface	Specifies to show the interface DHCPv6 Client configuration and running information. If **interface** is not entered, the command will show the device DUID.
INTERFACE-NAME	Specifies the identifier of the interface on the device to show the DHCPv6 client configuration and running information. If *INTERFACE-NAME* is not entered, the command output will be for all IPv6 interfaces.

Default None

Command Mode User EXEC

Usage Guideline The **show ipv6 dhcp** command shows the DHCP for IPv6 client configuration and running information of the specified interface. If the **interface** argument is not presented, the DHCPv6 Client DUID will be showed.

Examples The following example shows the DHCPv6 client's DUID:

```
Switch > enable
Switch # show ipv6 dhcp
This device's DHCPv6 unique identifier (DUID):
0001000111A8040D001FC6D1D47B.
```

The following example shows the DHCPv6 client for interface vlan1, when vlan1 is DHCPv6 client disabled:

```
Switch > enable
Switch # show ipv6 dhcp interface vlan1
Switch #
```

The following example shows the DHCPv6 client for interface vlan1, when vlan1 is in the REQUEST state:

```
Switch > enable
Switch # show ipv6 dhcp interface vlan1
Interface vlan1 is in DHCPv6 client mode.
General prefix: aaa
State: REQUEST
Server IP: N/A
Server DUID: N/A
Preference: 0
Event expire: 10
IA is not acquired.
```

The following example shows the DHCPv6 client for interface vlan1, when vlan1 is in the ACTIVE state:

```
Switch > enable
Switch # show ipv6 dhcp interface vlan1
Interface vlan1 is in DHCPv6 client mode.
General prefix: aaa
State: ACTIVE
Server IP: fe80::21d:92ff:fe2b:af48%vlan1
Server DUID: 0001000611D6EE73001D922BAF48
Preference: 87
IA Type: PD
IA ID: 0003
T1: 300
T2: 800
Prefer Lifetime: 3600
Valid Lifetime: 7200
Prefix: 3000:1:2::/48
IA expire: 299
Addr expire: 7199
```

The following example shows the DHCPv6 client for interface vlan1, when vlan1 is in the RENEW state:

```
Switch > enable
Switch # show ipv6 dhcp interface vlan1
Interface vlan1 is in DHCPv6 client mode.
General prefix: aaa
State: RENEW
Server IP: fe80::21d:92ff:fe2b:af48%eth0
Server DUID: 0001000611D6EE73001D922BAF48
Preference: 87
Event expire: 17
IA Type: PD
IA ID: 0003
T1: 300
T2: 800
Prefer Lifetime: 3600
Valid Lifetime: 7200
Prefix: 3000:1:2::/48
IA expire: 219
Addr expire: 5119
```

The following example shows the DHCPv6 client for interface vlan1, when vlan1 is in the REBIND state:

```
Switch > enable
Switch # show ipv6 dhcp interface vlan1
Interface vlan1 is in DHCPv6 client mode.
General prefix: aaa
State: REBIND
Server IP: fe80::21d:92ff:fe2b:af48%eth0
Server DUID: 0001000611D6EE73001D922BAF48
Preference: 87
Event expire: 26
IA Type: PD
IA ID: 0003
T1: 300
T2: 800
Prefer Lifetime: 3600
Valid Lifetime: 7200
Prefix: 3000:1:2::/48
Addr expire: 3192
```

show ipv6 dhcp relay interface

These commands are used to display DHCP relay information.

show ipv6 dhcp relay interface *VLAN-interface*

Syntax Description	
VLAN-interface	Specific VLAN interface name.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline The **show ipv6 dhcp relay** command shows the DHCP for IPv6 relay configuration and running information of the specified VLAN interface.

Example The following example shows the DHCPv6 client for interface vlan1, when vlan1 DHCPv6 relay enabled

```
Switch > enable
Switch # show ipv6 dhcp relay interface vlan1
Listen interface name: vlan1
Sever Addsess FE80::2:3
Destination interface name: vlan2
```

show ipv6 general-prefix

This command is used to display IPv6 general prefix information. It is used the show ipv6 general-prefix command.

show ipv6 general-prefix [*PREFIX-NAME* **]**

Syntax Description	
PREFIX-NAME	The name of the general prefix to be showed. If the general prefix name is not specified, then all general prefixes on the system will be showed. The general prefix name can be 1-16 characters.

Default None

Command Mode User EXEC

Usage Guideline Use the **show ipv6 general-prefix** command to view information on IPv6 general prefixes.

Examples The following example shows how to display all IPv6 general prefixes on the swtch:

```
Switch > enable
Switch # show ipv6 general-prefix
IPv6 prefix dhcp-prefix
  Acquired via DHCP Client:
    vlan1
  Apply to interface:
    vlan3
      ::3:3:3:3:3/64
    vlan2
      ::4:4:4:4:4/64
      ::2:2:2:2:2/64
IPv6 prefix my-prefix
  Acquired via Manual configuration:
    3ffe:1:1::/48
  Apply to interface:
    vlan2
      ::1:1:1:1:1/64
```

The following example shows how to display information for a specified general prefix named my-prefix:

```
Switch > enable
Switch # show ipv6 general-prefix my-prefix
IPv6 prefix my-prefix
  Acquired via Manual configuration:
    3ffe:1:1::/48
  Apply to interface:
    vlan2
      ::1:1:1:1:1/64
```

show ipv6 interface

These commands are used to display IPv6 interface information.

show ipv6 interface [IFNAME]

Syntax None

Default None

Command Mode EXEC mode or any configuration mode.

Usage Guideline If the IPv6 address DAD fail, the IPv6 address is marked "DAD check fail"

Example This example shows how to display IPv6 interface incidence:

```
Switch > enable
Switch # show ipv6 interface vlan1
  vlan1 is down,
  IPv6 is disable
 link-local address is :
    fe80::a01:2ff:fe39:1
  global unicast address is :
    3ffe:501:ffff:100:a01:2ff:fe39:1/64 (DAD check fail)
  MAC Address is 08-01-02-39-00-01
  IP MTU is 1500 bytes
  IPv6 Hop Limit is 64
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised is sending
  ND advertised reachable time is 604151836 milliseconds
  ND advertised retransmit interval is 257243264 milliseconds
  ND router advertisements are sent between 604143192 to 5 seconds
  ND router advertisements live for 54212 seconds
  Hosts use stateless autoconfig for addresses.

Switch #
```

show ipv6 interface brief

These commands are used to display IPv6 interface summary information.

show ipv6 interface IFNAME brief

Syntax None

Default None

Command Mode EXEC mode or any configuration mode.

Usage Guideline The [status/protocol] information is the same description with "show ip interface brief" command in the "Basic IPv4 command Reference Doc".

An IPv6 interface can be in either down state or up state. As an interface is in up state, it can send and receive packets. If an interface is in down state, the directly connected routing entry is removed from the routing table. Removing the entry allows the software to use dynamic routing protocols to determine backup routes to the network.

If you specify an optional interface type, you see information for that specific interface. At current stage, the supporting interface type is VLAN.

If you specify no optional arguments, you see information on all the interfaces.

If the interface hardware is usable, the interface is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.

If the IPv6 address DAD fail, the IPv6 address is marked "DAD check fail"

Example This example shows how to display IPv6 interface brief incidence:

```
Switch > enable
Switch #show ipv6 interface brief
lo                          [up/up]
    unassigned
vlan1                       [up/up]
    2010:312::1
    fe80::a01:2ff:fe39:1
vlan2                       [up/up]
    2010:311::1 (DAD check fail)
Switch #
```

show ipv6 neighbors

This command is used to display the IPv6 neighbor information.

show ipv6 neighbors

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline None

Example The example shows how to display IPv6 neighbor information.

```
Switch > enable
Switch # show ipv6 neighbors
IPv6 Address                    MAC Address       Interface   Type   Status
fe80::250:baff:fef9:b512        0050.baf9.b512    vlan1       DYNM   STALE

Switch #
```

Display Field Descriptions Description of significant display fields.

Display Field	Description
Type	DYNM - Dynamic learning entry. STATIC - Static neighbor entry (for example, user configuration) LOCAL - Local interface entry.
Status	REACH (Reachable) - Positive confirmation was received within the last ReachableTime, in milliseconds, that the forward path to the neighbor was properly functioning . While in the REACH state, the device takes no special action as packets are sent. STALE - More than the ReachableTime, in milliseconds, has elapsed since the last positive confirmation was received that the forward path was properly functioning. While in the STALE state, the device takes no action until a packet is sent. DELAY - More than ReachableTime, in milliseconds, has elapsed since the last positive confirmation was received that the forward path was properly functioning. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within the DELAY_FIRST_PROBE_TIME in seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE. PROBE - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer, in milliseconds.

show ipv6 ospf

To display general information about OSPF routing processes, use the **show ipv6 ospf** command.

show ipv6 ospf [*PROCESS-ID***]**

Syntax Description	
PROCESS-ID	(Optional) Internally used identification parameter for an IPv6 OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each IPv6 OSPF routing process.

Default If the *PROCESS-ID* is not specified, display all IPv6 OSPF processes.

Default *PROCESS-ID*: null

Command Mode User EXEC

Usage Guideline The information displayed by the **show ipv6 ospf** command is useful in debugging OSPF routing operations.

Example The following is sample output from the **show ipv6 ospf command.**

```
Switch > enable
Switch # show ipv6 ospf
```

The output after executing this command is as follows on the next page.

```
Routing Process "OSPFv3 null" with Operational Router 10.76.37.30
Process uptime is 0DT0H13M51S.
Conforms to RFC 2740
This router is an ABR; ABR Type is Standard (OSPFv3).
This router is an ASBR (injecting external routing information).
This router is a BR.
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
Number of router LSA 5. Checksum Sum 0x22263
Number of netwrok LSA 1. Checksum Sum 0xE8A7
Number of inter-area prefix LSA 16. Checksum Sum 0x92112
Number of inter-area router LSA 1. Checksum Sum 0x26DD
Number of external LSA 0. Checksum Sum 0x0000
Number of link LSA 3. Checksum Sum 0x15A79
Number of intra-area prefix LSA 5. Checksum Sum 0x34475
Number of LSA originated 18
Number of LSA received 13
Number of current LSA 31
LSDB database overflow limit is 12288
Number of areas in this router is 3
Area 0.0.0.0 (BACKBONE) (active)
Number of interfaces in this area is 1 active interface number is 1
Number of fully adjacent virtual neighbors through this area is 0
SPF algorithm last executed 0DT0H12M39S
SPF algorithm executed 4 times
Number of LSA 13. Checksum Sum 0x616B2
Area 0.0.0.1 (active)
Number of interfaces in this area is 1 active interface number is 1
Number of fully adjacent virtual neighbors through this area is 1
SPF algorithm last executed 0DT0H12M39S
SPF algorithm executed 5 times
Number of LSA 8. Checksum Sum 0x4E6DD
Area 0.0.0.3 (active)
Number of interfaces in this area is 1 active interface number is 1
Number of fully adjacent virtual neighbors through this area is 0
SPF algorithm last executed 0DT0H13M29S
SPF algorithm executed 2 times
Number of LSA 7. Checksum Sum 0x499DF
```

show ipv6 ospf border-routers

To display the ABRs and ASBRs for the IPv6 OSPF process, use the **show ipv6 ospf border-routers** command.

show ipv6 ospf [*PROCESS-ID***] border-routers**

Syntax Description	
PROCESS-ID	(Optional) Internally used identification parameter for an IPv6 OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each IPv6 OSPF routing process.

Default None

Command Mode User EXEC

Usage Guideline Use this command to display the ABRs and ASBRs information.

If *PROCESS-ID* is not specified, display all IPv6 OSPF processes.

Example This is a sample output from the show ipv6 ospf border-routers command.

```
Switch > enable
Switch # show ipv6 ospf border-routers
```

The result after executing this command is as follows.

```
OSPFv3 Routing Table (Process null)
Codes: i - Intra-area route, I - Inter-area route
i 47.65.49.111 [1] is directly connected, vlan49, ABR, Area 0.0.0.0
Total Entries: 1
```

show ipv6 ospf database

Display the database summary of the OSPF routing processes, use the **show ipv6 ospf database** command.

show ipv6 ospf [*PROCESS-ID***] database [router | network | inter-prefix | inter-router | external | link | intra-prefix] [adv-router [self-originate |** *ROUTER-ID***]]**

Syntax Description	
PROCESS-ID	(Optional) Internally used identification parameter for an IPv6 OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each IPv6 OSPF routing process
ROUTER-ID	(Optional) Router ID can be specified as either a decimal value or as an IPv4 address.

Default None

Command Mode User EXEC

Usage Guideline A router's collection of LSA data is stored in a link-state database. The contents of the database, when subjected to the Dijkstra algorithm, result in the creation of the OSPF routing table.

Both of these keywords can be appended to all other keywords used with the **show ipv6 ospf database** command to provide more detailed information.

If the *PROCESS-ID* argument is not specified, display all IPv6 OSPF processes.

Example The following is sample output from the **show ipv6 ospf database** command when no arguments or keywords are used.

```
Switch > enable
Switch # show ipv6 ospf database
OSPFv3 Router with ID (20.0.1.10) (Process null)
Link-LSA (Interface vlan1)
ADV Router      Age  Seq#       CkSum   LinkCnt
20.0.1.10        1053 0x80000001 0xaf9f      1

 Router-LSA (Area 0.0.0.0) (BACKBONE)

ADV Router      Age  Seq#       CkSum   LinkCnt
20.0.1.10        1013 0x80000002 0x34dd      0
```

show ipv6 ospf interface

To display OSPF-related interface information, use the **show ipv6 ospf interface** command.

show ipv6 ospf interface ***[****IFNAME****]***

Syntax Description	
IFNAME	(Optional) Interface type and number. If no option is specified, applying the command displays the entire IPv6 OSPF process.

Default None

Command Mode User EXEC

Usage Guideline None.

Example show ipv6 ospf interface Standard Output Example: The following is sample output from the show ipv6 ospf interface command.

```
Switch > enable
Switch # show ipv6 ospf interface
```

The result after executing this command is as follows.

```
vlan2 is up, line protocol is up
  Interface ID 1026
  IPv6 Prefixes
    fe80::a01:2ff:fe36:2/64 (Link-Local Address)
    3ffe:4::30/64
  OSPFv3 Process (null), Area 0.0.0.1 (active)
  MTU 1500, Instance ID 0
    Router ID 10.76.37.30, Network Type BROADCAST, Cost: 1 (default)
    Transmit Delay is 1 sec, State BDR, Priority 1
    Designated Router (ID) 10.76.37.3
      Interface Address fe80::219:5bff:fef5:2cc1
    Backup Designated Router (ID) 10.76.37.30
      Interface Address fe80::a01:2ff:fe36:2
    Timer intervals configured, Hello 10, Dead 40, Retransmit 5
      Hello due in 0DT0H0M5S
    Neighbor Count is 1, Adjacent neighbor count is 1
    Hello received 48 sent 46, DD received 5 sent 3
    LS-Req received 1 sent 1, LS-Upd received 11 sent 10
    LS-Ack received 8 sent 6, Discarded 00
```

show ipv6 ospf neighbor

To display IPv6 OSPF neighbor information on a per interface basis, use the **show ipv6 ospf neighbo**r command.

show ipv6 ospf [*PROCESS-ID*] neighbor [*IFNAME* | *NEIGHBOR-ID*] [detail]

Syntax Description	
PROCESS-ID	(Optional) Internally used identification parameter for an IPv6 OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each IPv6 OSPF routing process.
IFNAME	(Optional) Interface type and number. If no option is specified, the command applies to the entire IPv6 OSPF process.
NEIGHBOR-ID	(Optional) Neighbor ID. It can be specified as either a decimal value or as an IPv4 address.
detail	(Optional) Displays all neighbors in detail; lists all neighbors.

Default None

Command Mode User EXEC

Usage Guideline The keywords can be appended to all other keywords used with the **show ipv6 ospf neighbor** command to display the information desired.

Example The following is sample output from the **show ipv6 ospf neighbor** command with the detail keyword.

```
Switch > enable
Switch # show ipv6 ospf neighbor
```

The result after executing this command is as follows.

```
The result after executing this command is as follows.
OSPFv3 Process (null)
Neighbor ID     Pri   State           Dead Time     Interface  Instance ID
10.76.37.3        1   Full/DR           0DT0H0M33S    vlan2      0
10.76.37.3        1   Full/ -           0DT0H0M38S    VLINK1     0
Total Entries: 2
```

show ipv6 ospf route

To display the current contents of the IPv6 OSPF routing table, use the **show ipv6 ospf route** command.

show ipv6 ospf [*PROCESS-ID***] route**

Syntax Description	
PROCESS-ID	(Optional) Internally used identification parameter for an IPv6 OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each IPv6 OSPF routing process.

Default None

Command Mode User EXEC

Usage Guideline The information displayed by the **show ipv6 ospf route** command is useful in debugging OSPF routing operations.

If *PROCESS-ID* is not specified, the command will display all IPv6 OSPF processes.

Example The following is sample output from the **show ipv6 ospf route** command.

```
Switch > enable
Switch # show ipv6 ospf route
OSPFv3 Process (null)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
O  3ffe:1::/64                                      11
     via fe80::219:5bff:fef5:2cc1, vlan2, TransitArea 0.0.0.1
O  3ffe:2::/64                                       1
     directly connected, vlan2, TransitArea 0.0.0.1
O  3ffe:2::10/128                                    1
     via fe80::219:5bff:fef5:2cc1, vlan2, TransitArea 0.0.0.1
C  3ffe:3::/64                                       1
     directly connected, vlan3, Area 0.0.0.3
C  3ffe:4::/64                                       1
     directly connected, vlan2, TransitArea 0.0.0.1
C  3ffe:4::30/128                                    0
     directly connected, vlan2, TransitArea 0.0.0.1
Total Entries: 6 entries, 6 routes
```

show ipv6 ospf virtual-links

To display parameters and the current state of IPv6 OSPF virtual links, use the **show ipv6 ospf virtual-links** command.

show ipv6 ospf [*PROCESS-ID*] virtual-links

Syntax Description	
PROCESS-ID	(Optional) Internally used identification parameter for an IPv6 OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each IPv6 OSPF routing process.

Default None

Command Mode User EXEC

Usage Guideline The information displayed by the show ipv6 ospf virtual-links command is useful in debugging OSPF routing operations.

If *PROCESS-ID* is not specified, the command will display all IPv6 OSPF processes.

Example The following is sample output from the **show ipv6 ospf virtual-links** command.

```
Switch > enable
Switch # show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 10.76.37.3 is up
  Transit area 0.0.0.1 via interface vlan2, instance ID 0
  Local address 3ffe:4::30/128
  Remote address 3ffe:2::10/128
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
    Hello due in 0DT0H0M2S
    Adajcency state Full
```

show ipv6 protocols [PROCESS-ID ospf | rip]

Use this command to display the parameters and current state of the active IPv6 OSPF or RIP routing protocol processes.

show ipv6 protocols [*PROCESS-ID* **ospf | rip]**

Syntax Description	
PROCESS-ID	(Optional) Internally used identification parameter for an IPv6 OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each IPv6 OSPF routing process.
ospf	(Optional) Display OSPFv3 global settings which are related to the overall IP routing function.
rip	(Optional) Display RIPng global settings which are related to the overall IP routing function.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline The information displayed by the show ipv6 protocols command is useful in debugging routing operations. The output can help to identify a router suspected of delivering faulty routing information.

The information displayed by the show ipv6 protocols rip command is useful in debugging routing operations.

If no option is specified, the summary of all of running routing protocols will be displayed .

Examples The following is sample output from the **show ipv6 protocols ospf** command.

```
Switch > enable
Switch # show ipv6 protocols ospf
Routing Protocol is "ospfv3 null"
Configured Router ID : auto
Redistribute route default metric: auto
Auto-cost Reference-bandwidth: 100
Distance: (default is 110)
Don't originate type 5 default route
Redistributing:
type metric metric_type
-------------------------------------
connected 20 2
static 20 2
rip 20 2
```

The following is sample output from the **show ipv6 protocols rip** command.

```
switch#show ipv6 protocols rip
Routing Protocol is "ripng"
  Sending updates every 30 seconds with +/-50%, next due in 1 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Default redistribute metric is 1
  Redistributing:
    type            metric
    ---------------------------------------

  Interface:
    vlan2
    vlan3

  Routing for Networks:
    vlan2 : 3ffe:4::30/64
    vlan3 : 3ffe:3::30/64
  max. no. of IPv6 RIP routes allowed: 6144
  no. of IPv6 RIP routes excluding connected: 2

  Distance:
    distance (default)120
```

show ipv6 rip database

To display information about current IPv6 RIP processes, use the **show ipv6 rip database** command.

show ipv6 rip database

Syntax Description	
database	If specifed the command displays the details of the entries in the specified RIP IPv6 routing table.

Default None

Command Mode User EXEC

Usage Guideline The information displayed by the **show ipv6 rip database** command is useful when debugging RIPng routing operations.

Examples The following is sample output from the **show ipv6 rip database** command.

```
Switch > enable
Switch # show ipv6 rip database
```

The result after executing this command is as follows.

```
Codes: R - RIP, Rc - RIP connected, Rs - RIP static,
       K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP

   Network                 Next Hop                If       Met  Time
R  3ffe:1::/64               fe80::219:5bff:fef5:2cc1  vlan2      2
0DT0H2M31S
R  3ffe:2::/64               fe80::219:5bff:fef5:2cc1  vlan2      2
0DT0H2M31S
Rc 3ffe:3::/64               ::                        vlan3      1
Rc 3ffe:4::/64               ::                        vlan2      1

Total Entries: 4 entries, 4 routes
```

show ipv6 rip interface

To display the usability status of interfaces configured for IPv6 RIP, use the **show ipv6 rip interface** command.

show ipv6 rip interface [*IFNAME***]**

Syntax Description	
IFNAME	The specified interface type and interface number

Default None

Command Mode User EXEC

Privileged EXEC mode Usage Guideline

Use the **show ipv6 rip interface** command to validate the IPv6 RIP status of an interface and its configured addresses. The **show ipv6 rip interface** command also displays the parameters that IPv6 RIP is using on this interface including any configured features.

If the argument *IFNAME* is not used then all IPv6 RIP interfaces are displayed.

Example The following is sample output in vlan1 from the **show ipv6 rip interface** command.

```
Switch > enable
Switch # show ipv6 rip interface vlan1
vlan1 is up, line protocol is up
    Routing Protocol: RIPng
           Passive interface: Disabled
           Split horizon: Enabled with Poisoned Reversed
           IPv6 interface address:
             fe80::a01:2ff:fe36:1/64
```

show ipv6 route

Use this command **show ipv6 route** to display the active IPv6 routes in the system.

show ipv6 route [*IPV6-ADDRESS* **[** *INTERFACE-TYPE INTERFACE-NUMBER* **|** *NEXT-HOP-ADDRESS* **] |** *NETWORK-PREFIX I PREFIX-LENGTH* **[** *INTERFACE-TYPE INTERFACE-NUMBER* **|** *NEXT-HOP-ADDRESS* **] | [database]** *PROTOCOL* **| [database] connected | [database] static]**

Syntax Description	
NETWORK-PREFIX	(Optional) The IPv6 network that is the destination of the static route.
PREFIX-LENGTH	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
IPV6-ADDRESS	(Optional) Displays routing information for a specific IPv6 address.
PROTOCOL	(Optional) The name of a routing protocol, specify a routing protocol, use one of the following keywords: ospf and rip.
INTERFACE-TYPE	(Optional) Interface type. For more information about supported interface types, use the question mark (?) to access the online help function.
INTERFACE-NUMBER	(Optional) Interface number. For more information about the numbering syntax for supported interface types, use the question mark (?) to access the online help function.
database	(Optional) the routing database is shown and the active route populated in the forwarding database is prefixed with an asterisk.
connected	(Optional) All connected local interface routes.
static	(Optional) All static routes.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline When the system provides forwarding services for IPv6 traffic, it is very important and helpful to check the forwarding/routing table to understand what the current traffic path is in the network.

Example

Use the **show ipv6 route** command to check what are the active routing entries for IPv6 .

```
Switch > enable
Switch # show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - IS-IS, B - BGP
S ::/0 [1/0] via 192:0:7:2::2
C 20:50:71:1::/64 is directly connected, vlan10
O 115:50:70::/64 [110/2] via fe80::a00:1ff:fe02:6, vlan10, 0DT0H0M7S
O 150::/64 [110/20] via fe80::a00:1ff:fe02:6, vlan10, 0DT0H0M7S
C 192:0:7:2::/64 is directly connected, vlan111
S 192:0:123:2::/64 [1/0] via 20:50:71:1::2
[1/0] via 192:0:7:2::2
S 192:0:244:2::/64 [1/0] via 20:50:71:1::2
S a100::/64 [1/0] via fe80::250:baff:fe91:bb28, vlan111
[1/0] via fe80::a00:1ff:fe02:6, vlan10
Total Entries: 8 entries, 10 routes
Switch #
```

Use the **show ipv6 route database** command to check which routing database entries for IPv6 are currently working.

```
Switch > enable
Switch # show ipv6 route database
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP
       > - selected route, * - FIB route, p - stale info

S*> ::/0 [1/0] via 192:0:7:2::2
O   20:50:71:1::/64 [110/1] vlan10, 0DT0H8M36S
C*> 20:50:71:1::/64 is directly connected, vlan10
O*> 115:50:70::/64 [110/2] via fe80::a00:1ff:fe02:6, vlan10, 0DT0H1M5S
O*> 150::/64 [110/20] via fe80::a00:1ff:fe02:6, vlan10, 0DT0H1M5S
O   192:0:7:2::/64 [110/1] vlan111, 0DT0H8M36S
C*> 192:0:7:2::/64 is directly connected, vlan111
S*> 192:0:123:2::/64 [1/0] via 20:50:71:1::2
 *>                  [1/0] via 192:0:7:2::2
S*> 192:0:244:2::/64 [1/0] via 20:50:71:1::2
S*> a100::/64 [1/0] via fe80::250:baff:fe91:bb28, vlan111
 *>           [1/0] via fe80::a00:1ff:fe02:6, vlan10

Total Entries: 10 entries, 12 routes
```

show ipv6 route summary

To display the current state of the IPv6 routing table, use the **show ipv6 route summary** command.

show ipv6 route summary

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline None

Example The following is sample output from the **show ipv6 route summary** command:

```
Switch#show ipv6 route summary
IPv6 routing table name is Default-IPv6-Routing-Table(0)
IPv6 routing table maximum-paths state is enabled
IPv6 routing table configured maximum-paths is 6
IPv6 routing table maximum-paths is 6
Route Source Networks
connected       4
static          1
rip             34
Total           39
FIB             34
multi-path      0
```

show loopback-detection

Use the command to show the current loopback detection control settings.

show loopback-detection [interface [INTERFACE-ID] [, | -]

Syntax

<cr>	To show all the loopback detection protocol information.
Interface *INTERFACE-ID*	Specify the interface-ID which you want to display.
,	(Optional) Specify a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specify a range of interfaces. No space before and after the hyphen.
detail	(Optional) Displays detailed information about the spanning-tree state.

Default None

Command Mode EXEC mode or any configuration mode

Usage Guideline Show the loopback detection information.

Example This example shows current loopback detection setting and running status for port-based mode.

```
Switch# show loopback-detection
Status          : Enabled
Mode            : Port-Based
Interval        : 20 s

Interface     LoopDetect State      Result            Time Left(sec)
------------- --------------------- ----------------- --------------
eth3.1        Enabled               Normal
eth3.8        Enabled               Normal
eth4.5        Enabled               Loop              20
```

This example shows current loopback detection setting for vlan-based mode.

```
Switch# show loopback-detection
Status          : Enabled
Mode            : VLAN-Based
Interval        : 20 sec

Interface     LoopDetect State     Result               Time Left(sec)
------------- -------------------- -------------------- ---------------
eth3.1        Enabled               Normal
eth3.8        Enabled               Normal
eth4.5        Enabled               Loop on Vlan 2          120
                                    Loop on Vlan 3          115
```

This example shows all interface settings.

```
Switch# show loopback-detection interface
Interface     Loopdetect Mode      Loop Status         Time Left(sec)
------------- -------------------- ------------------ -------------
eth3.1        Enabled               Normal
eth3.8        Enabled               Normal
eth4.5        Enabled               Loop                20

Total Entries: 3
Switch#
```

show logging

Use **show logging** to display the state of the system logging process and the contents of the standard system logging buffer.

show logging [host | buffer [*START-INDEX* **[** *STOP-INDEX* **] |**

+ *VALUE* **| -** *VALUE* **]]**

Syntax Description	
host	(Optional) Displays the logging hosts.
buffer	(Optional) Only display the content of system logging buffer.
START-INDEX	(Optional) The logging index number to start the display from.
STOP-INDEX	(Optional) The logging index number to stop the display at. If both the *START-INDEX* and *STOP-INDEX* are not specified, all logs in the system logging buffer will be displayed. If only *START-INDEX* is specified, the logs after the start index number (included) will be displayed.
+ *VALUE*	(Optional) Using this argument paired with the number of messages (*VALUE* a positive integer) will display the indicated number of first messages in the buffer.
- *VALUE*	(Optional) Using this argument paired with the number of messages (*VALUE* a positive integer) will display the indicated number of last messages in the buffer.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use this command to check the current settings of the system logging process and view the logs in the system logging buffer.

If the keywords, **host** or **buffer** are not specified, then the switch only displays general information about the state of system logging and the logging host table.

Examples The following page shows an example of the command **show logging** with the keyword **host**:

```
DGS-6600:15(config)#show logging host

Host         Severity       Facility     Port
-------------------------------------------------------
30.65.45.34  informational  local7       514
35.4.56.2    critical       local4       1300

DGS-6600:15(config)#show logging

logging on :enabled
logging buffer severity:notice

Host         Severity       Facility     Port
-------------------------------------------------------
30.65.45.34  informational  local7       514
35.4.56.2    critical       local4       1300
```

Below is an example of using the + *VALUE* and - *VALUE* arguments with the **show logging buffer** command:

```
DGS-6600:15#show logging buffer + 3

Total logs:401

Index Date                  Log Text
-------------------------------------------------------------------------------
3     12:12:04, 2010-08-14  Interface eth4.47 is up

2     12:12:04, 2010-08-14  Interface vlan99 is up

1     12:11:47, 2010-08-14  System is cold started

DGS-6600:15#show logging buffer - 3

Total logs:401

Index Date                  Log Text
-------------------------------------------------------------------------------
401   06:26:45, 1993-01-03  Successfully login to the system by user anonymous,

IP 0.0.0.0, via console at privilege level 2

400   06:26:35, 1993-01-03  System is cold started

399   14:05:03, 2010-12-13  System is rebooted by user admin, IP 0.0.0.0, via co

nsole
```

Below is an example of using the *START-INDEX* and *STOP-INDEX* arguments with the **show logging buffer** command.

```
DGS-6600:15(mgmt-if)# show logging buffer 250 260

Total logs:402

Index Date                  Log Text
------------------------------------------------------------------------
--
260   08:53:15, 2010-09-20  Interface vlan1 is down

259   08:53:14, 2010-09-20  Interface eth4.47 is up

258   08:53:14, 2010-09-20  Interface vlan1 is up

257   08:45:08, 2010-09-20  eth4.1 state change from LRN to FWD for MSTID 0

256   08:45:08, 2010-09-20  eth4.1 state change from BLK to LRN for MSTID 0

255   08:45:07, 2010-09-20  eth4.43 state change from LRN to FWD for MSTID 0

254   08:45:07, 2010-09-20  eth4.43 state change from BLK to LRN for MSTID 0

253   08:45:05, 2010-09-20  Interface eth4.1 is up

252   08:45:05, 2010-09-20  Interface vlan99 is up

251   08:45:04, 2010-09-20  Interface eth4.43 is up

250   08:45:04, 2010-09-20  Interface vlan20 is up

DGS-6600:15(mgmt-if)#
```

show mac address-table

Use the **show mac address-table** command to display: a specific MAC address, static entries, dynamic entries or the MAC address table of static and dynamic entries for a specific physical interface, port-channel or VLAN.

show mac address-table [dynamic | static] [address *MAC-ADDR* **| interface [** *INTERFACE-ID* **[, | -] | vlan** *VLAN-ID* **]**

Syntax Description	
dynamic	(Optional) Displays dynamic MAC address table entries only.
static	(Optional) Displays static MAC address table entries only.
address *MAC-ADDR*	Specifies the 48-bit MAC address; the valid format is XX:XX:XX:XX:XX:XX
interface *INTERFACE-ID*	Display information for a specific interface. Valid interfaces include physical ports and port-channels.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline None

Examples This is an example of output from the show mac address-table address command:

```
Switch# show mac address-table address 00:02:4B:28:C4:82
Vlan Mac Address       Type    Ports
---- ----------------- ------- -----------------------
   1 00-02-4b-28-c4-82 Static  CPU
Total Entries: 1
```

This is an example of output from the **show mac address-table static** command:

```
Switch> show mac address-table static
Vlan Mac Address       Type    Ports
---- ----------------- ------- -------------------------
   1 01-00-0c-cc-cc-cc Static  CPU
   1 01-80-c2-00-00-00 Static  CPU
   1 01-00-0c-cc.cc-cd Static  CPU
   1 01-80-c2-00.00-01 Static  CPU
   1 01-80-c2-00.00-04 Static  CPU
   1 01-80-c2-00.00-05 Static  CPU
   4 00-01-00-02.00-04 Static  eth3.2
   6 00-01-00-02.00-07 Static  eth3.1
Total Entries : 8
Switch#
```

This is an example of output from the **show mac address-table address** on interface VLAN 1:

```
Switch# show mac address-table vlan 1
Vlan Mac Address       Type    Ports
---- ----------------- ------- -------------------------
   1 00-02-4B-28-C4-82 Static  CPU
   1 00-03-40-11-22-33 Dynamic eth3.2
```

show mac address-table aging destination-hit

Use the **show mac address-table aging destination-hit** command to display the status of destination MAC address triggered update function.

show mac address-table aging destination-hit

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline None

Examples This is an example of output from the **show mac address-table aging destination-hit** command:

```
Switch> show mac address-table aging destination-hit
Mac address-table aging destination-hit is enabled
```

show mac address-table aging-time

Use the **show mac address-table aging-time** command to display the aging time.

show mac address-table aging-time

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline None

Example This is an example of output from the **show mac address-table aging-time** command:

```
Switch> show mac address-table aging-time
Aging Time is 300 seconds.
```

show mgmt-if

Use this command to show the status of the management port, including user settings and link status.

show mgmt-if

Syntax Description None

Default None

Command Mode User EXEC, management interface mode or any configuration mode

Usage Guideline None

Example This example shows how to display the status of the management port.

```
Switch#show mgmt-if
Management Interface
------------------------
Admin Status: Down
IPv4 Address: 10.1.1.1/8
IPv4 Default Gateway : 10.1.1.254
IPv6 Global Address     : 6600::66/64
IPv6 Link-local Address : fe80::40b:ff:fe19:0/64
IPv6 Default Gateway    : ::
IP MTU          : 1600
Link Status : Down
Switch#
```

show monitor session

Use this command to show all or a specific port mirroring session.

show monitor session [*SESSION-NUMBER* | *remote* | *local* **]**

Syntax Description

SESSION-NUMBER	(Optional) Specify the session number which you want to display.
local	(Optional) Specify to display local session.
remote	(Optional) Specify to display remote RSPAN session.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline If the command is entered without specifying a session number, all port mirroring sessions are displayed.

Examples This example shows how to display a created port mirroring session with session number 1.

```
Switch# show monitor session 1
Session 1
Session Type: local session
Destination Port : eth3.1
Ingress Disable
Source Ports :
        Both : eth3.2-3.4
         RX : eth3.5
         TX : eth3.7
Switch#
```

This example shows how to display all the created port mirroring sessions.

```
Switch# show monitor session
Session 1
   Session type: local session
Destination Port  : eth1.1
Source Ports      :
Both : eth1.2-4
RX   : eth1.5
TX   : eth1.7

Session 2
   Session type: local session
Destination Port  : eth2.1
Source Ports      :
Both : eth2.2-4
RX   : eth1.5
TX   : eth1.7
Session 3
   Session type: remote source session
Destination remote VLAN  : VLAN 100
Source Ports      :
Both : eth2.2-4
RX   : eth1.5
TX   : eth1.7
Session 4
   Session type: remote destination session
source remote VLAN  : VLAN 100
destination Ports   : eth2.5

Switch#
```

show multicast filtering-mode

Use the **show multicast filtering-mode** command to display the filtering mode for handling the multicast packets received on the interface.

show multicast filtering-mode [interface *INTERFACE-ID***]**

Syntax Description	
INTERFACE-ID	(Optional) Specifies the interface to display the filtering mode on (only VLAN interfaces are supported).

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Only VLAN interfaces support multicast filtering-mode configuration.

Examples This is an example of output from the **show multicast filtering-mode** for all vlan interfaces.:

```
Switch> show multicast filtering-mode
Interface           Multicast Filtering Mode
---------           ------------------------
VLAN1               filter-unregistered
VLAN2               filter-unregistered
VLAN3               filter-unregistered
VLAN4               filter-unregistered
VLAN5               forward-unregistered
VLAN6               forward-unregistered
VLAM7               forward-unregistered
VLAN8               forward-unregistered
VLAN9               forward-unregistered
VLAN10               forward-unregistered
Total Entries: 10
Switch>
```

This is an example of output from the **show multicast filtering-mode** for the vlan 1 interface:

```
Switch> show multicast filtering-mode interface vlan1
Interface           Multicast Filtering Mode
---------           ------------------------
VLAN1               filter-unregistered
Total Entries: 1
```

show policy-map

Use this command to display the policy map configuration.

show policy-map [*POLICY-NAME* **| interface** *INTERFACE-ID***]**

Syntax Description	
INTERFACE-ID	(Optional) Module and port number.
POLICY-NAME	(Optional) Specifies the name of the policy map. If not specified, all policy maps will be displayed.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline The **show policy-map** command displays the class policies configured for the policy map. Use the show policy-map command to display all class policy configurations comprising any existing service policy map.

The command **show policy-map** *INTERFACE-ID* displays the policy map configuration if the service policy has been attached to the specified interface.

Examples The following is sample output from the **show policy-map** command. As shown below, in the policy map called policy1, two-rate traffic policing has been configured for the class called police. Two-rate traffic policing has been configured to limit traffic to an average committed rate of 500 Mbps and a peak rate of 1 Gbps.

```
Switch(config)#class-map police
Switch(config-cmap)#match access-list acl_rd
Switch(config-cmap)#policy-map policy1
Switch(config-pmap)#class police
Switch(config-pmap-c)#police cir 500000 bc 10000 pir 1000000 be 10000
exceed-action set-dscp-transmit 2 violate-action drop
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#interface eth3.1
Router(config-if)#service-policy policy1
Router(config-if)#end
```

The following sample output shows the contents of the policy map called policy1:

```
Switch# show policy-map policy1
Policy Map policy1
Class police
police tr-tcm cir 500000 bc 10000 pir 1000000 be 10000 exceed-action : set-dscp-transmit 2
 violate-action : drop
Total Entries : 1
```

The following sample output shows all policy maps configured at eth3.1:

```
Switch# show policy-map interface eth3.1
Policy Map: policy1
Class police
police tr-tcm cir 500000 bc 10000 pir 1000000 be 10000 exceed-action : set-dscp-transmit 2
 violate-action : drop
Total Entries : 1
```

show port-security

Use this command to display the current port security setting.

show port-security [interface *INTERFACE-ID* **[, | -]] [address]**

Syntax Description	
INTEFACE-ID	(Optional) Specifies the ID of interfaces to display.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.
address	(Optional) Display all the secure MAC addresses including both of configured and learned entries.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline If no interface ID is specified, the **show port-security** command will display the port security setting of all existing port interfaces.

If the mac-address **address** option is specified, the configured and learned secure MAC address entries will be displayed.

If no optional keyword is specified with **show port-security** command, all of the port-security information is displayed.

Examples This example shows how to display the port security setting of interface port eth4.1.

```
DGS-6600:15#show port-security interface eth4.1

Interface     Max No.  Current No.  Violation  Secure Type        State
-------------------------------------------------------------------------
eth4.1          1         0         Shutdown   Delete-on-Timeout  Disabled

Total Entries: 1
```

show power-saving

Use this command to display the power saving information.

show power-saving

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline None

Example The following example shows how to display power-saving information.

```
DGS-6600:2#show power-saving

Power-saving status
===========================
phy power-saving:Enabled
```

show qos aggregate-policer

Use this command to display the configured aggregated policer.

show qos aggregate-policer [*NAME***]**

Syntax Description	
NAME	(Optional) Specifies the name of the aggregate policer.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline None

Example This example shows how to display the aggregate policer.

```
Switch> show qos aggregate-policer
   QoS policy aggregate : agg-policer5
    rate:64 burst-normal: 128
          exceed-action : drop
   QoS policy aggregate : agg-policer6
tr-tcm cir 64 bc 128 pir 256 be 512
          exceed-action : set-dscp-transmit 2
         violate-action : drop
Total Entries:2
```

show qos interface

Use this command to display the port level QoS configurations.

show qos interface *INTERFACE-ID* **[,|-] { cos | deficit-round-robin | trust | bandwidth | dscp-mutation | map {dscp-color | cos-color | dscp-cos} }**

Syntax Description	
interface *INTERFACE-ID***[,|-]**	Specifies the interface ID to display. Specify multiple interface IDs, which are separated by a comma (,) or hyphen (-). No space is before or after the comma or hyphen.
cos	Displays the port default CoS.
deficit-round-robin	Displays the DRR configuration.
trust	Displays the port trust state.
bandwidth	Displays the bandwidth limitation configured for the port.
dscp-mutation	Displays the DSCP mutation map attached to the interface.
map dscp-color	Displays the DSCP to color map.
map cos-color	Displays the CoS to color map.
map dscp-cos	Displays the mapping of DSCP to CoS.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline If no keywords are specified after **show qos**, then the summary of QoS settings will be shown.

Examples This example displays the default CoS for ports eth3.2 - eth3.5.

```
Switch> show qos interface eth3.2-3.5 cos
Interface  CoS
---------- ----
eth3.2      3 (qos)
eth3.3      4 (qos)
eth3.4      4 (qos)
eth3.5      3 (qos)

Total Entries: 4
```

This example displays the port trust state for ports eth3.2 - eth3.5.

```
Switch> show qos interface eth3.2-3.5 trust
Interface   Trust State
---------- ------------
eth3.2     trust DSCP
eth3.3     trust CoS
eth3.4     trust DSCP
eth3.5     trust CoS

Total Entries: 4
Switch>
```

The following example displays the deficit round robin configuration for ports eth3.1- eth3.2:

```
Switch> show qos interface eth3.1-3.2 deficit-round-robin
eth3.2
  CoS  Quantum (Kbytes)
  ----  --------------
  0       16
  1       32
  2       16
  3       32
  4       16
  5       64
  6       64
  7       strict priority

eth3.2
  DRR is disabled.

Switch>
```

This example displays the DSCP mutation maps attached to ports eth3.1 to 3.2.

```
Switch> show qos interface eth3.1-3.2 dscp-mutation
Interface   DSCP Mutation Map
----------  ------------------
eth3.1       Mutate Map 1
eth3.2       Mutate Map 2
Total Entries: 2
```

The following example displays the CoS bandwidth allocation for ports eth3.1-3.2:

```
Switch> show qos interface eth3.1-3.2 bandwidth

Bandwdith Control Table

Interface Ingress Rate (Kbps) Egress Rate (Kbps)
-------------------------------------------------
eth3.1       64 (qos)           128 (qos)
eth3.2       256 (dot1x)        256 (dot1x)

Total Entries: 2
```

This example displays the DSCP to color map for ports eth3.1 to eth3.2.

```
Switch> show qos interface eth3.1-3.2 map dscp-color
eth3.1
   DSCP 0-7,44-63 are mapped to Green
   DSCP 41-43 are mapped to Yellow
   DSCP 8-40 are mapped to Red
eth3.2
   DSCP 0-63 are mapped to Green


Total Entries: 2
```

This example displays the CoS to color map for ports eth3.3 to eth3.4.

```
Switch> show qos interface eth3.3-3.4 map cos-color
eth3.3
   CoS 0-2,5,7 are mapped to Green
   CoS 3-4 are mapped to Yellow
   CoS 6 are mapped to Red
eth3.4
   CoS 0-7 are mapped to Green

Total Entries: 2
```

The following example displays the DSCP to CoS map for ports eth3.1.

```
Switch> show qos interface eth3.1 map dscp-cos eth3.1
   0  1  2  3  4  5  6  7  8  9
--------------------------------
00 00 00 00 00 00 00 00 01 01
10 01 01 01 01 01 01 02 02 02 02
20 02 02 02 02 03 03 03 03 03 01
30 03 03 04 04 04 04 04 04 04 04
40 05 05 05 05 05 05 05 05 06 06
50 06 06 06 06 06 06 07 07 07 07
60 07 07 07 07
```

show qos map

Use this command to display the QoS DSCP mutation map configuration.

show qos map dscp-mutation [*MAP-NAME***]**

Syntax Description	
MAP-NAME	(Optional) Specifies the name of the DSCP mutation map to display.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline If no name is specified after show qos map dscp-mutation, all maps will be displayed.

Example The following example displays the global DSCP mutation map.

```
Switch> show qos map dscp-mutation
DSCP Mutation: mutemapl
Attaching interface:
eth2.1, eth2.2, eth2.3, eth2.4, eth2.5, eth3.1, eth3.2, eth3.3, eth3.4,
eth3.5, eth3.6, eth3.7, eth3.8, eth3.9,eth3.10
   0  1  2  3  4  5  6  7  8  9
--------------------------------
00 00 01 02 03 04 05 06 07 08 09
10 10 11 12 13 14 15 16 17 18 19
20 20 21 22 23 24 25 26 27 28 29
30 30 31 32 33 34 35 36 37 38 39
40 40 41 42 43 44 45 46 47 48 49
50 50 51 52 53 54 55 56 57 58 59
60 60 61 62 63
```

show route-map

Use this command to display static route maps,

show route-map [*MAP-NAME***]**

Syntax Description	
MAP-NAME	(Optional) Name of a specific route map.

Default None

Command Mode Privileged EXEC

Usage Guideline The command displays all the ACL-specific information that pertains to the route map in the same display without having to execute a **show route-map** command to display each ACL that is associated with the route map.

Example This example shows how to display static route maps for the entry "myPolicy"

```
Switch# show route-map myPolicy
route-map myPolicy, permit, sequence 10
  Match clauses:
    as-path R1
  Set clauses:
    weight 120
Switch#
```

show running-config

Use this command to display the contents of the current running configuration file.

show running-config

Syntax None

Default None

Command Mode Privilege EXEC at level 15

Usage Guideline The **show running-config** command output for the current running system configuration. .

Example The following example shows how to display the contents of the current running configuration file:

```
Switch:15(config)#show running-config
Building configuration...
Current configuration:
version 1.00.001


#Slot Module-Type                          Model
#---- ------------------------------------ -------------
# 1    Management Control Module          CMU-Card
# 2    -                                    -
# 3    -                                    -
# 4    48 ports 1000Base-T                48T-IOCard
!
!
!
```

show snmp

Use this command to display the SNMP information of the device.

show snmp { community | host | view | group | engineID }

Syntax Description	
community	Display SNMP community information.
host	Display SNMP trap recipient information.
view	Display SNMP view information.
group	Display SNMP group information.
engineID	Display SNMP local engine ID information.

Default None

Command Mode Privileged EXEC or any configuration mode

Usage Guideline This command displays the SNMP information.

Examples This example shows how to display SNMP community information.

```
Switch# show snmp community
Codes: ro - read only, rw - ReadWrite

(rw)System
(ro)public
(ro)Develop
(rw)private

Total Entries: 4
```

This example is sample output from the command **show snmp host**.

```
Switch# show snmp host
Host IP Address       SNMP Version        Community Name            SNMPv3 User Name
--------------------  ------------------  ------------------------  ----------------
10.48.76.100          v3 noauth                                      initial
10.51.17.1            v2c                 public
20:64:84::154         v2c                 public

Total Entries: 3
Switch#
```

This example is sample output from the command **show snmp view**.

```
Switch# show snmp view
View Name              Subtree                    View Type
-------------------------------------------------
restricted             1.3.6.1.2.1.1              Included
restricted             1.3.6.1.2.1.11             Included
restricted             1.3.6.1.6.3.10.2.1         Included
restricted             1.3.6.1.6.3.11.2.1         Included
restricted             1.3.6.1.6.3.15.1.1         Included
CommunityView          1                          Included
CommunityView          1.3.6.1.6.3                Excluded
CommunityView          1.3.6.1.6.3.1              Included

Total Entries: 8
Switch#
```

This example is sample output from the command **show snmp group**.

```
Switch# show snmp group
groupname: ILMI                    security model:v1
readview :*ilmi                 writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                       security model:v2c
readview : *ilmi                    writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: public                       security model:v1
    readview : <no readview specified>  writeview: <no writeview specified>
notifyview: *tv.FFFFFFFF.FFFFFFFF.FFFFFFF0F
row status: active

groupname: public                       security model:v2c
readview : <no readview specified> writeview: <no writeview specified>
   notifyview: *tv.FFFFFFFF.FFFFFFFF.FFFFFFF0F
row status: active
Total Entries: 4
Switch#
```

This example is sample output from the command **show snmp engineID**.

```
Switch# show snmp engineID
Local SNMP engineID: 000000090200000000C025808
Switch#
```

show snmp-server

Use this command to display configuration information about the SNMP server.

show snmp-server [traps]

Syntax Description	
traps	(Optional) Display the control for all trap notifications.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use this command to display the global configuration about the SNMP server without using the keyword **traps**. When the keyword **traps** is specified, the state control for all trap notifications will be shown.

Examples This example shows how to display the SNMP server configuration

```
Switch# show snmp-server
SNMP Server   : Enabled
System Name : DGS-XXXXS Stackable Switch
Location      : HQ 15F
Contact       : MIS Department II
```

This example shows how to display the state control for all traps notification

```
Switch# show snmp-server traps
Global Trap State : Enabled
SNMP
Authentication         : Enabled
linkup                 : Enabled
linkdown               : Enabled
coldstart              : Enabled
warmstart              : Disabled
bridge                    : Enabled
rmon                      : Disabled
entity                    : Disabled
vrrp                      : Enabled
ping                      : Disabled
traceroute                : Disabled
equipment                 : Disabled
agent                     : Enabled
mstp                      : Disabled
pkt-storm-ctrl            : Disabled
safe-guard                : Disabled
single-ip                 : Disabled
mac-violation             : Disabled
mac-notificaiton          : Disabled
```

show snmp user

Use this command to display information about the configured characteristics of an SNMP user.

show snmp user [*USER-NAME* **]**

Syntax Description	
USER-NAME	(Optional) Name of a specific user or users about which to display SNMP information.

Default None

Command Mode Privileged EXEC or global configuration

Usage Guideline An SNMP user must be part of an SNMP group, as configured using the **snmp-server user** *USER-NAME GROUP-NAME* command. When the username argument is not entered, the **show snmp use**r command displays information about all configured users.

Example This example shows how to display the SNMP user authuser's information.

```
Switch# show snmp user authuser
User Name: authuser
Engine ID: 000000090200000000C025808
Authentication Protocol: MD5
Privacy Protocol: DES
Group Name: VacmGroupName
Total Entries: 1
```

Display Field Descriptions Description of significant display fields.

Display Field	Description
User Name	A string identifying the name of the SNMP user.
Engine ID	Per snmp user's engineID is copied from the local system engineID.
Authentication Protocol	Identifies which authentication protocol is used. Options are message digest algorithm 5 (MD5), Secure Hash Algorithm (SHA) packet authentication, or None
Privacy protocol	Indicates whether Data Encryption Standard (DES) packet encryption is enabled.
Group Name	Indicates the SNMP group the user is a part of. • SNMP groups are defined in the context of a View-based Access Control Model (VACM).

show sntp

Use this command to show information about the SNTP server.

show sntp

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline None

Example The following example shows how to display the SNTP information:

```
Switch> show sntp
SNTP server    Version    Last Receive
------------   -------    ------------
171.69.118.9         5          00:01:02
172.21.28.34         4          00:00:36     Synced
Total Entries: 2.
Switch>
```

show spanning-tree

This command is used to show the information about the STP module. This command is only for STP & RSTP.

show spanning-tree [interface [*INTERFACE-ID* **[, | -]]**

Syntax Description	
interface *INTERFACE-ID*	Specifies the *INTERFACE-ID* which to display information for.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and after the hyphen.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Show the Spanning-Tree Configuration for the single spanning tree when in RSTP/ STP-compatible mode.

Issuing the command without any argument displays all the spanning-tree protocol information.

An error message will appear when the operating mode is MSTP.

Examples The example on the next page shows how to display the spanning information.

```
Switch# show spanning-tree
Spanning tree: Enabled, mode: RSTP
Forwarding BPDU : Disabled
Root ID    Priority      : 4097
           Address       : 00-04-9B-78-08-00
Bridge ID  Priority      : 4097 (priority 4096 sys-id-ext 1)
           Address       : 00-04-9B-78-08-00
           Hello Time    : 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
 Topology Changes Count : 0

 codes - F: Fast forwarding is configured as enabled
         Configured link type: A- Auto, P- point to point, S- shared
                                          Priority  Link
   Interface  Role       State      Cost    .Port    Type        Edge
   ---------  -----      -----      ------  --------- ------      --------
FA eth3.3     designated forwarding 20000     128.3   p2p         edge
FA eth3.5     backup     blocking   200000    128.5   p2p         non-edge
 A eth3.6     backup     blocking   200000    128.6   shared      edge
 P eth3.7     root       forwarding 2000      128.9   p2p         edge

Total Entries: 4
Switch#
```

This example shows how to display spanning configuration information for a specific interface.

```
Switch#show spanning-tree interface eth4.7
eth4.7
  STP                          : Enabled
  Priority                     : 128
  Port Role                    : Root
  Port State                   : Forwarding
  Configured Fast-Forwarding: Auto,    Operation status : None-Edge
  Configured Link Type         : Auto,   Operation status: P2P
  Configured Path Cost         : Auto,   Operation result: 200000
  Guard Root                   : Disabled
  TCN Filtering                : Disabled
Switch#
```

show spanning-tree mst

Use the command to show the information that used in MSTP version.

show spanning-tree mst [configuration [digest]]

show spanning-tree mst [instance *INSTANCE-ID* **[, | -]]**

show spanning-tree mst [instance *INSTANCE-ID* **[, | -] interface** *INTERFACE-ID* **[, | -]]**

Syntax Description	
configuration	Specifies to display a table of the mapping relationship between VLANs and MSTP Instances.
digest	Specifies to display the MD5 digest included in the current MST configuration identifier (MSTCI).
instance *INSTANCE-ID* **[, | -]**	Specifies to show the MSTP information for the designated instance only. Multiple instances can be defined. Use ',' to specify a series of instances, or separate a range of instances from a previous range. Or use '-' to specify a range of instances. No space before and after the comma or hyphen.
interface *INTERFACE-ID* **[, | -]**	Show the MSTP information for the specified interface. Multiple interfaces can be defined. Use ',' to specify a series of interfaces, or separate a range of interfaces from a previous range. Or use '-' to specify a range of interface. No space before and after the comma or hyphen.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline MSTP-specific information is only displayed by this command, and this command is applicable only when the MSTP mode is enabled.

Issuing the command without any argument will show all the MSTP specific information.

An error message will appear if the operating mode is STP or RSTP.

Examples This example shows how to MSTP summary information.

```
Switch# show spanning-tree mst
Spanning tree: Enabled, protocol:MSTP
Operation status: Forward delay 15 sec, Max age 20 sec
Configured      : Forward delay 15 sec, Max age 20 sec,
                  max hops 20, transmit hold count 6

>>>>>MST0 vlans mapped:   1,4-4094
Bridge Address: 00-12-85-26-05-00,  priority: 32768 (32768 sysid 0)
Designated Root Address: 00-54-85-26-05-00, Priority: 4096  (4096 sysid 0)
Regional Root: this swtich
Designated Bridge: this switch



codes - F: Fast forwarding is configured as enabled,
        Configured Link type: A - Auto, S- Shared,P- Point to point
                                                Priority  Link
   Interface   Role         State        Cost    .Port#    Type    Edge
   ----------  ----------   ----------   ------  --------- ------  --------

FA eth3.3      designated   forwarding   20000   128.3     p2p     edge
FA eth3.5      backup       blocking     200000  128.5     p2p     non-edge
 A eth3.6      backup       blocking     200000  128.6     shared  edge
 A eth3.7      root         forwarding   2000    128.9     p2p     edge

>>>>MST02 vlans mapped:   2-3
Bridge address:00-12-d9-87-47-00 , priority: 32770 (32768 sysid 2)
Designated Root : this switch for MST2
Regional Root: MST02
Designated Bridge: MST02
                                                Priority  Link
   Interface   Role         State        Cost    .Port#    Type    Edge
   ----------  ----------   ----------   ------  --------- ------  --------
FA eth3.9      designated   forwarding   20000   128.9     p2p     edge
 P eth3.10     backup       blocking     200000  128.10    p2p     non-edge
 A eth3.11     backup       blocking     200000  128.11    shared  edge
 A eth3.12     root         forwarding   2000    128.12    p2p     edge
Switch#
```

This example shows how to display the MSTP MD5 digest information.

```
Switch#show spanning-tree mst digest
Name     : [region1]
Revision : 2, Instances configured: 3
Digest   : 3C 60 DB F2 4B 03 EB F0 9C 59 22 F4 56 D1 8A 03
Switch#
```

show ssh

Use this command to display the status of Secure Shell (SSH) server connections.

show ssh

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use the **show ssh** command to display the status of the SSH connections on the switch. This command does not display any SSH configuration data; use the **show ip ssh** command to display SSH configuration information such as timeouts and retries.

Example This example shows how to display SSH connections information.

```
Switch# show ssh
SID  Ver. Cipher                 Userid                          Host
--------------------------------------------------------------------------------
0    V2   aes256-cbc/hmac-sha1   admin                       126.100.51.22
Switch#
```

Display Field Descriptions Description of significant display fields.

Display Field	Description
SID	A unique number that identifies the SSH session.
Ver	Indicates the SSH version of this session.
Cipher	The crypto / Hashed Message Authentication Code (HMAC) algorithm that the SSH client is using.
Userid	The login username that has been authenticated for the session.
Host	The IP address of the system running an SSH client.

show startup-config

Use this command to display the content of the startup configuration file.

show startup-config

Syntax None

Default None

Command Mode Privilege EXEC at level 15

Usage Guideline Use **show startup-config** command to display the system configuration contents of the file which is specified with the **boot config** command. If no boot config command is applied, the factory default system configuration content is displayed.

Example The following example shows how to display the content of the startup system configuration file:

```
Switch:15(config)#show startup-config
#Boot configuration file=flash:\configurations\def_usr.conf
#Switch Chassis-based High-Speed Switch
#Firmware Version:1.00.001
```

show storm-control

Use this command to show the current storm control settings.

show storm-control [interface [*INTERFACE-ID*] [, | -] [broadcast | multicast | unicast]]

Syntax Description	
INTERFACE-ID	Interface name/id.
broadcast	Displays the current Broadcast storm setting
multicast	Displays the current Multicast storm setting
unicast	Displays the current Unicast (DLF) storm setting

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline If the *INTERFACE-ID* is specified, the storm control settings of the specified interface will appear on the screen.

If no *INTERFACE-ID* is specified, then the configurations of all interfaces will appear.

If no traffic type is specified, then all types of storm control settings will appear.

If there is no configuration on the interface specified, the interface will not be displayed,

Examples This example shows the current Broadcast storm control setting.

```
Switch# show storm-control interface broadcast

  Interface   Storm          Action    Type               Threshold
  ----------- -------------- --------- ------------------ --------------
  eth3.1      Broadcast      Drop      pps                500
  eth3.2      Broadcast      Shutdown  percentage         80
  eth3.3      Broadcast      Shutdown  percentage         80

Total Entries:3
```

This example shows all the interface settings.

```
Switch# show storm-control interface

  Interface   Storm          Action       Type              Threshold
  ----------- -------------- ------------ ----------------- ---------------
  eth3.1      Broadcast      Drop         pps               500
  eth3.1      Multicast      Drop         percentage        80
  eth3.1      Unicast        Drop         percentage        80
  eth3.2      Broadcast      Shutdown     percentage        90
  eth3.2      Multicast      Drop         percentage        80
  eth3.3      Broadcast      Shutdown     percentage        85

Total Entries: 6
```

This example shows the interface settings for the range from port eth3.1 to eth3.2.

```
Switch# show storm-control interface eth3.1-3.2

  Interface   Storm          Action       Type              Threshold
  ----------- -------------- ------------ ----------------- ---------------
  eth3.1      Broadcast      Drop         pps               500
  eth3.1      Multicast      Drop         percentage        80
  eth3.1      Unicast        Drop         percentage        80
  eth3.2      Broadcast      Shutdown     percentage        90
  eth3.2      Multicast      Drop         percentage        80

Total Entries: 5
```

This example shows the global settings.

```
Switch# show storm-control

Time Interval       : 15  seconds
Countdown Timer     :  180 seconds
Auto Recover Time   :  300 seconds
```

show system

Use this command to display information about the Switch system.

show system [cpu] [protocol-state]

Syntax Description	
cpu	(Optional) Shows the information about the CPU utilization of the management control unit.
protocol-state	(Optional) Shows the information about supporting protocols.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline This command displays information about the overall Switch system. Use keyword of protocol-state to show the information about the administrative and operational state of the supported protocols.

Example This example on the following page shows how to display the Switch information

```
Switch>show system

 Device Type                    :Chassis-based High-Speed Switch
 Hardware Version               :A1
 First MAC Address              :06:B0:00:17:00:00
 Number of MAC Address(es)      :4096

Slot: 1
 Hardware Version               :0A1G
 Bootloader Version             :1.00.002
 Firmware Version               :1.00.018
 S/N                            :QT0X1AC000001
 Model Name                     :DGS-6600-CMI
 First MAC Address              :06:60:0c:10:00:20
 Number of MAC Address(es)      :1


Slot: 2
 Hardware Version               :0A0-2
 Bootloader Version             :1.00.002
 Firmware Version               :1.00.018
 S/N                            :QT101AC000001
 Model Name                     :DGS-6600-48P
 First MAC Address              :08:03:04:37:00:00
 Number of MAC Address(es)      :48


Slot: 3
 Hardware Version               :0A0-1
 Bootloader Version             :1.00.002
 Firmware Version               :1.00.018
 S/N                            :QT111AC000001
 Model Name                     :DGS-6600-48TS
 First MAC Address              :08:03:05:21:00:00
 Number of MAC Address(es)      :48


Slot: 4
 Hardware Version               :0A1G
 Bootloader Version             :1.00.002
 Firmware Version               :1.00.018
 S/N                            :QT0Z1AC000001
 Model Name                     :DGS-6600-48S
 First MAC Address              :06:48:c0:14:00:00
 Number of MAC Address(es)      :48
```

The following shows the output for the command **show system protocol-state** command:

```
DGS-6600:15#show system protocol-state
Password Encryption              :Disabled
SNMP Server                      :Disabled
SNMP6 Server                     :Disabled
Sys Logging                      :Enabled
TELNETv4                         :Enabled(TCP:23)
TELNETv6                         :Enabled(TCP:23)
WEB                              :Enabled(TCP:80)
SSH                              :Disabled(TCP:22)
SSH6                             :Disabled(TCP:22)
RMON                             :Enabled
Spanning Tree Version            :Disabled
LACP                             :Enabled
802.1x                           :Disabled
GVRP                             :Disabled
ERPS                             :Disabled
RIP                              :Disabled
OSPF                             :Disabled
BGP                              :Disabled
Multicast Routing                :Disabled
DVMRP                            :Enabled
PIM-DM                           :Enabled
PIM-SM                           :Enabled
IGMP Snooping                    :Enabled
IGMP                             :Enabled
DHCPv4 Relay                     :Disabled
DHCPv4 Client                    :Enabled
DHCPv4 Server                    :Disabled
AAA Authorization                :Disabled
VLAN Tunnel                      :Disabled
Voice VLAN                       :Disabled
RIPng                            :Disabled
OSPFv3                           :Disabled
IPv6 DHCP Relay                  :Enabled
IPv6 DHCP Client                 :Enabled
VRRP                             :Enabled
sFlow                            :Disabled
Loopback Detection               :Disabled
LLDP                             :Disabled
DHCP Server Screening            :Enabled
DHCP Snooping                    :Disabled
IP Source Guard                  :Disabled
Dynamic ARP Inspection           :Disabled
Policy Base Route                :Enabled
DGS-6600:15#
```

show time-range

Use this command to display the time range profile configuration.

show time-range [*NAME* **]**

Syntax Description	
NAME	(Optional) The name of the time-range profile to be displayed. If no *NAME* argument is specified, all time-range profiles will be displayed. Up to 32 characters are allowed.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline None

Example This example shows how to display the content of the configured time range profile, named trange1.

```
Switch(config)#show time-range trange1
time range name : trange1
09:00 ~ 12:00, every day
00:00 ~ 23:59, every Sat
00:00 ~ 23:59, every Sun
19:00 (the 1st day) ~ 17:00 (the 2nd day) every month
```

show traffic-segmentation

Use this command to show the traffic segmentation for some ports or all ports.

show traffic-segmentation [interface *INTERFACE-ID* **[, | -]]**

Syntax Description	
interface *INTERFACE-ID*	(Optional) Specifies the ID of an interface. The allowable interfaces are either physical ports or port channels.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline The allowable interface types for this command are either physical ports or port channels.

If entering **show traffic-segmentation** without any keywords, then the traffic segmentation configuration for all ports is displayed. Otherwise, only the specified interface's traffic-segmentation is shown.

Example This example shows the configuration of traffic segmentation for eth3.1

```
Switch# show traffic-segmentation interface eth3.1
Interface     Forwarding Interface(s)
--------------------------------------
eth3.1       eth3.1, eth3.4, eth3.5, eth3.6
Total Entries: 1
```

show unit

Use this command to display information about the system's modules.

show unit [*UNIT-ID* **]**

Syntax Description	
UNIT-ID	(Optional) Slot ID to indicate which slot (module) the information is going to be displayed for.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline This command displays information about the system's modules. If no option is specified, then all of the slots (modules) information are displayed.

Example This example shows how to display the information about the system's modules:

Note: The display text and format may differ depending on the SW release.

```
Slot Model             Status   Up-Time
---- ------------      -------- -------------
1    DGS-6600-CM       ok       0DT0H2M49S
2    -                 -        -
3    -                 -        -
4    DGS-6600-8XG      ok       0DT0H2M17S

Slot Model             Description
---- ------------      ------------------------------------------------------------
1    DGS-6600-CM       CPU/Fabric Management Module
2    -                 -
3    -                 -
4    DGS-6600-8XG      8-port 10GE XFP Module


     DRAM                           FLASH
Slot Total      Used      Free      Total     Used      Free
---- ---------  --------- --------- --------- --------- ---------
1    2074160k   1183436k  890724k   994952k   125656k   869296k
2    -          -         -         -         -         -
3    -          -         -         -         -         -
4    516012k    476924k   39088k    -         -         -
```

Display Field Descriptions Description of significant display fields.

Display Field	Description
up time	The operating time since system power-up.

show username

Use this command to display the username and password pair database.

show username [*NAME***]**

Syntax Description	
NAME	(Optional) A specfied name of a user account. Only one word is allowed for the name arguement. If no NAME is specified, all user accounts will be displayed.

Default None

Command Mode Privileged EXEC or any configuration mode; both at privilege level 15

Usage Guideline This command displays user accounts that have been created.

An error message will appear if the specified user does not exist.

Examples This example shows how to display all of the usernames configured in the switch.

```
Switch# show username
Password Encryption : Disabled

Username                  Access Level       Password                    Encrypted
-------------------------------------------------------------------------------
Admin                              15   mypassword
dlink                              15   *@&cRDtpNCeBiq15KOQsKVyrA0sAiCIZQwq   *

Total Entries: 2
Switch#
```

The table below describes the significant fields shown in the display.

Field	Description
Encrypted	'*' denotes the entry's password is encrypted. If there is no '*' next to the entry it indicates the password is 'Plain Text'.

show user-session

Use this command to display information about the active lines on the switch.

show user-session [console | telnet | ssh | http | https]

Syntax Description	
console	(Optional) displays the information of the current console users.
telnet	(Optional) displays the information of the current telnet users.
ssh	(Optional) displays the information of the current ssh users.
http	(Optional) displays the information of the current http users.
https	(Optional) displays the information of the current https users.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline This command displays the line number, connection name, hosts (including virtual access interfaces), idle time, and terminal location. An asterisk (*) indicates the current terminal session.

When no option specified, users accessing all interfaces will be displayed.

Example This example shows how to display all session information.

```
Switch# show user-session

UI Codes: co - console, h - http, hs - https, s - ssh, te -telnet

ID   Login Time            From              UI  Level        Username
-------------------------------------------------------------------------
-----
* 0  01:12:23, 2008-05-13  0.0.0.0           co  15 12345678901234567890
  1  01:00:28, 2008-05-13  172.171.160.100   te  15 admin

Total Entries: 2
```

show version

To display version information about software, hardware, etc., use the **show version** command.

show version

Syntax None

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline This command displays the software and hardware information about the Switch.

Example This example shows how to display the software and hardware versions on a DGS-6604 switch:

```
Switch#show version
GS-6604  System Version

Backplane H/W version:0A1G   PCBA version:0   CPLD version:15
Serial#: 123456789-123456789-123456789-0123456789

Slot   Module Type    Versions
------ ------------- ------------------------------------------------
--
1      DGS-6600-CM    Serial#:     P4Z21A9000001
                      H/W:         0A1G
                      Bootloader:  1.00.001
                      PCBA:        0
                      Runtime:     1.00.021
                      CPLD:        ver-0

2      -              -
3      -              -
4      DGS-6600-48S   Serial#:     123456789-123456789-123456789-0123456789
                      H/W:         0A1G
                      Bootloader:  1.00.001
                      Runtime:     1.00.021
                      CPLD:        ver-4
```

show vlan

Use the **show VLAN** command to display the parameters for all configured VLANs or one VLAN (if the VLAN id or name is specified) on the switch.

Use the command **show vlan subnet-base** or **show vlan mac-base** to display a subnet-based VLAN or MAC-based VLAN respectively.

Use the command **show vlan [subnet|mac]** to display a subnet-based VLAN or a MAC-based VLAN respectively.

show vlan [*VLAN-ID* **[, | -] interface [** *INTERFACE-ID* **[, | -]]] [dynamic | detail]**

show vlan [subnet-base | mac-base]

Syntax Description	
VLAN-ID	(Optional) Display information about a single VLAN identified by VLAN id number. The VLAN id range is 1 to 4094. Separate non-consecutive VLAN-IDs with a comma; use a hyphen to designate a range of VLAN-ID.
interface	(Optional) Displays the interface port's PVID, ingress checking, acceptable frame type information.
INTERFACE-ID	Specifies the port to display.
,	(Optional) Specifies a series of ports, or separate a range of ports from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of ports. No space before and after the hyphen.
[detail | **dynamic]**	(Optional) Specifies what kind of information to be displayed. The optional keywords are: **detail**: display detailed information including static and dynamic information about the specified VLAN(s) **dynamic**: display dynamic membership which is learned by GVRP for the specified VLAN(s). If neither detail nor dynamic is specified, only the static configuration will be shown.
subnet-base	(Optional) display subnet-based VLAN related configuration.
mac-base	(Optional) display mac-based VLAN related configuration.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use the **show vlan** command to display the current VLAN status. Show the VLAN list table using **show vlan** command. Show a specific VLAN entry using **show vlan** *VLAN-ID*. Use **show vlan interface** command to show port-oriented VLAN information, such as, port PVID, ingress checking, and acceptable frame type information.

The following are the causes for an interface to become an untagged member port of a VLAN.

1. Configuration using an access VLAN command.
2. VLAN assignment from a RADIUS server.

Use the command **show vlan [subnet-base | mac-base]** to display a Subnet-based VLAN or MAC-based VLAN respectively.

If no optional key word is specified all of VLAN configurations are displayed.

Examples

This example shows how to display all current VLAN entries.

```
Switch# show vlan

VLAN 1:
   Name: default
   GVRP advertisement: yes
   Static Tag Member Ports:
      None
   Static Untag Member Ports:
      eth4.2, eth4.3, eth4.4, eth4.5, eth4.6,
      eth4.7, eth4.8, eth4.9, eth4.10, eth4.11,
      eth4.12, eth4.13, eth4.14, eth4.15, eth4.16,
      eth4.17, eth4.18, eth4.19, eth4.20, eth4.21,
      eth4.22, eth4.23, eth4.24, eth4.25, eth4.26,
      eth4.27, eth4.28, eth4.29, eth4.30, eth4.31,
      eth4.32, eth4.33, eth4.34, eth4.35, eth4.36,
      eth4.37, eth4.38, eth4.39, eth4.40, eth4.41,
      eth4.42, eth4.44, eth4.45, eth4.46, eth4.48,
      port-channel1,
   GVRP Advertise Ports:
      eth4.1-eth4.48, port-channel1
   Forbidden Ports:
      None


VLAN 20:
   Name: VLAN0020
   GVRP advertisement: yes
   Static Tag Member Ports:
      eth4.47,
   Static Untag Member Ports:
      eth4.43,
   GVRP Advertise Ports:
      eth4.1-eth4.48, port-channel1
   Forbidden Ports:
      None
```

This example shows how to display information for interface ports eth4.1 to eth4.3. Information such as ingress checking and the acceptable frame type is displayed.

```
Switch# show vlan interface eth4.1-4.3
 eth4.1
 PVID                    : 99
 GVRP State              : Disabled
 Ingress checked         : Enabled
 Access VLAN             : 99
 Advertise VLAN          : 1-4094
 Forbidden VLAN          :
 Acceptable frame types  : admit-all

 eth4.2
 PVID                    : 1
 GVRP State              : Disabled
 Ingress checked         : Enabled
 Access VLAN             : 1
 Advertise VLAN          : 1-4094
 Forbidden VLAN          :
 Acceptable frame types  : admit-all

 eth4.3
 PVID                    : 1
 GVRP State              : Disabled
 Ingress checked         : Enabled
 Access VLAN             : 1
 Advertise VLAN          : 1-4094
 Forbidden VLAN          :
 Acceptable frame types  : admit-all

Switch#
```

This example shows how to display the MAC-base VLAN table.

```
Switch(config)#show vlan mac-base
MAC Address           VLAN ID
-----------------     -------
00-80-cc-00-00-11         100
00-80-cc-00-00-21         100
00-80-cc-00-00-12         200
00-80-cc-00-00-31         300
00-80-cc-00-00-33         300
Total Entries: 5
Switch(config)#
```

This example shows how to display the subnet-base VLAN table.

```
Switch(config)#show vlan subnet-base
Subnet            VLAN ID
----------        ------
20.0.1.0/8         100
192.0.1.0/8       100
20.0.2.0/8         200
20.0.3.0/8         300
Total Entries: 4
Switch(config)#
```

show vlan-tunnel

Use this command to display the VLAN tunnel related settings.

show vlan-tunnel [*INTERFACE-ID* **[, | -]]**

Syntax Description	
[*INTERFACE-ID* **[, | -]]**	(Optional) Multiple interfaces can be specified to be displayed. The multiple interface numbers are separated by comma, or hyphen. No spaces before and after the comma or hyphen. If no *INTERFACE-ID* is specified, VLAN tunnel settings on all interfaces are displayed. If no argument is specified only the status of VLAN tunnel mode will be shown.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Specify that the information displayed is about a specfic interface(s) in the VLAN translation table. If no argument is specified only the status of VLAN tunnel mode will be shown.

Examples This example shows how to display the status of VLAN tunnel mode.

```
Switch# show vlan-tunnel
VLAN tunneling: enabled

eth4.1:UNI port, CoS remarking: 5, ingress-checking: disabled,
remove-inner-tag: disabled
VLAN           S-VID C-VID  CoS
-------------  ----  -----  -------
encapsulation 1001   2002   5
                     2003   5
                     2004   5
encapsulation 1002   1002   5
                     2003   5
                     3004   6
remarking         2  102    4
remarking         3  103    5
remarking         4  104    5

eth4.2:NNI port, TPID:0x88a8

eth4.3:UNI port, CoS remarking: disabled, ingress-checking: enabled,
remove-inner-tag: disabled

VLAN           S-VID C-VID  CoS
-------------  ----  ----   -------
encapsulation 1001   2002   trusted
                     2003   trusted
                     2004   trusted
encapsulation 1002   1002   4
                     2003   5
                     3004   6
remarking        2    102   4
remarking        3    103   trusted
remarking        4    104   7
```

Display Field Descriptions The following table shows the detailed description for the above fields.

Field	Description
VLAN tunneling	The state of the VLAN tunneling function.
UNI port	Indicates that the port is either a UNI port or NNI port.

Field	Description
CoS remarking	Indicates the CoS remarking status at the port. It could be either disabled or an integer from 0~7 (indicating the remarking CoS Value).
VLAN	Shows the VLAN encapsulation and remarking pairs.
S-VID/C-VID	Indicates the service provider VLAN ID and customer VLAN ID of the VLAN tunneling pair.
CoS	The CoS remarking setting for the VLAN tunneling pair.

This example shows how to display the VLAN tunnel settings for eth4.1.

```
Switch# show vlan-tunnel eth4.1
VLAN tunneling: disabled

eth4.1:UNI port, CoS remarking:5, ingress-checking: disabled,
remove-inner-tag: disabled
VLAN           S-VID CVID   CoS
-------------  ----  -----  -------
encapsulation 1001   2002   5
                     2003   5
                     2004   5
encapsulation 1002   1002   5
                     2003   5
                     3004   6
remarking       2    102    4
remarking       3    103    5
remarking       4    104    5
Switch#
```

show vlan-tunnel ctag-mapping

This command is used to display the state of the dynamically learned customer VLAN tag mechanism and the static customer VLAN tag mappings.

show vlan-tunnel ctag-mapping { dynamic state | static }

Syntax Description	
dynamic state	Display the state of dynamic learned customer VLAN tag mechanism.
static	Display all static customer VLAN tag mappings.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use the **show vlan-tunnel ctag-mapping dynamic state** command to display the state of dynamically learned customer VLAN tag mechanism.

Use the **show vlan-tunnel ctag-mapping static** command to show each static customer VLAN tag mapping entries that user configured.

Examples This example shows how to display the state of dynamic learned customer VLAN tag mechanism.

```
Switch# show vlan-tunnel ctag-mapping dynamic state
Dynamic ctag-mapping for IPv4 : Disable
Dynamic ctag-mapping for IPv6 : Disable
Switch#
```

This example shows how to display the VLAN tunnel static customer VLAN tag mapping entries.

```
Switch# show vlan-tunnel ctag-mapping static
Destination IP                                C-VID
--------------------------------------------- -------
192.168.10.0/24                               233
192.168.20.0/24                               155
2011:254::/64                                 850
--------------------------------------------- -------
Total Entries: 3
Switch#
```

show vrrp

This command is used to view the VRRP status.

show vrrp [interface *INTERFACE-ID* **[** *VRID* **]]**

Syntax Description	
INTERFACE-ID	(Optional) The interface name of a configured IP interface. When the *INTERFACE-ID* is specified, the VRRP information that is related to the interface will be displayed.
VRID	(Optional) A configured virtual router identifier .When both *INTERFACE-ID* and *VRID* are specified, the VRRP information that is related to it will be displayed. The virtual router identifier is configured with the vrrp ip command. Range is 1 to 255.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline Use this command to view the VRRP information.

Examples On the following page is an example from show vrrp. There are 2 VRID, 7 and 8, configured in the interface vlan1, a VRID 5 configured in interface vlan2 and a VRID 1 configured in interface vlan3.

```
Switch#show vrrp
vlan1 - VRID 7
  State is Master
  Virtual IP address is 20.0.1.1
  Virtual MAC address is 00-00-5e-00-01-07
  Advertisement interval is 1 sec
  Preemption enabled
  Priority is 255
  Critical IP address is 0.0.0.0
  Master router is 20.0.1.1 (local)
  Master Down interval is 3.003 sec

vlan1 - VRID 8
  State is Master
  Virtual IP address is 20.1.1.2
  Virtual MAC address is 00-00-5e-00-01-08
  Advertisement interval is 1 sec
  Preemption disabled
  Priority is 200
  Critical IP address is 0.0.0.0
  Master router is 20.0.1.1 (local)
  Master Down interval is 3.218 sec

vlan2 - VRID 5
  State is Initialize
  Virtual IP address is 30.1.1.254
  Virtual MAC address is 00-00-5e-00-01-05
  Advertisement interval is 1 sec
  Preemption enable
  Priority is 100
  Critical IP address is 70.5.1.1
  Master router is unknown
  Master Down interval is 3.609 sec

vlan3 - VRID 1
  State is Backup
  Virtual IP address is 50.1.1.254
  Virtual MAC address is 00-00-5e-00-01-01
  Advertisement interval is 1 sec
  Preemption disabled
  Priority is 80
  Critical IP address is 0.0.0.0
  Master router is 50.0.1.2
  Master Down interval is 3.687 sec (expires in 3.550 sec)
```

The following example shows how to view VRRP information of interface vlan1 and VRID 8.

```
Switch#show vrrp interface vlan1 8
vlan1 - VRID 8
  State is Master
  Virtual IP address is 20.1.1.2
  Virtual MAC address is 00-00-5e-00-01-08
  Advertisement interval is 1 sec
  Preemption disabled
  Priority is 200
  Critical IP address is 0.0.0.0
  Master router is 20.0.1.1
  Master Down interval is 3.218 sec
```

show vrrp brief

This command is used to view the VRRP brief status.

show vrrp brief [all]

Syntax Description	
all	(Optional) Displays all information for all virtual routers, including virtual routers in a shutdown state.

Default None

Command Mode User EXEC or any configuration mode

Usage Guideline When using the **show vrrp brief** command the status and parameter information for the configured VRRPs is displated in tabular format.

Example Below is the output of using the **show vrrp brief** command to view the brief VRRP information.

```
Switch#show vrrp brief
Interface VRID Prio Time     Own Pre State   Master Addr      VRouter Addr
vlan1     7    255  3.003     Y   Y  Master  20.0.1.1         20.0.1.1
vlan1     8    200  3.218         Y  Master  20.0.1.1         20.1.1.2
vlan2     5    100  3.609         Y  Init    0.0.0.0          30.1.1.254
vlan3     1    80   3.687         Y  Backup  50.0.1.2         50.1.1.254
```

The following table describes the fields in the **show vrrp brief** command output.

Field	Description
Interface	Interface name
VRID	Virtual router identifier
Prio	VRRP priority value
Time	Master down interval in seconds
Own	Indicates whether the virtual router is the IP address owner. "Y" indicates it is IP address owner.
Pre	Indicates preempt mode is enabled or not. "Y" indicates preempt mode is enabled.
State	State of the virtual router
Master Address	IP address of the master virtual router.
VRouter Address	IP address of the virtual router.

shutdown (interface)

Use this command to disable the port interface. Use the no form of the command to enable the port interface.

shutdown

no shutdown

Syntax None

Default Enabled

Command Mode Interface configuration

Usage Guideline Only physical port interfaces are valid for this configuration.

The command will change the state of a port to be disabled. In the disabled state, the port will not be able to receive or transmit any packets. Using the no shutdown command, the port will set the port to the enabled state. When a port is shutdown (disabled), the link status will also be off.

Examples Below demonstrates using the **shutdown** command to set interface port eth3.1 to the disabled state

```
Switch(config)# interface eth3.1
Switch(config-if)# shutdown
```

shutdown (Management Port)

Use this command to disable the management port. Use the no form of the command to turn the management port back to the enabled state.

shutdown

no shutdown

Syntax None

Default Enabled

Command Mode Management interface

Usage Guideline This command will disable the management port. Users cannot access or manage the system using the management port until the no shutdown command is executed.

Example Use the **shutdown** command to disable the Management Port.Verify the settings

```
Switch(config)#mgmt-if
Switch(mgmt-if)#shutdown
Switch(mgmt-if)#end
```

by entering the show mgmt-if command.

show ip dhcp snooping

Use this command to display DHCP snooping configuration.

show ip dhcp snooping

Syntax Not Applicable

Default Not Applicable

Command Mode EXEC mode or any configuration mode

Usage Guideline Use the command to display DHCP snooping configuration setting.

Example This example shows how to display DHCP Snooping configuration:

```
Switch# show ip dhcp snooping
DHCP Snooping is enabled.
DHCP Snooping is enabled on VLANs:
vlan10 vlan15 vlan16 vlan17 vlan18
Verify MAC address is Enabled
Information option: not allowed
Interface    Trusted
---------- ----------
eth3.1         no
eth3.8         no
eth3.9         yes


Switch#
```

show ip dhcp snooping binding

Use the command to display DHCP snooping binding entries.

show ip dhcp snooping binding [*IP-ADDRESS***] [***MAC-ADDRESS***] [***vlan VLAN-ID***] [***interface* **[***INTERFACE-ID* **[, | -]]]**

Syntax

IP-ADDRESS	(Optional) Display the binding entry based on IP address.
MAC-ADDRESS	(Optional) Display the binding entry based on MAC address.
vlan *VLAN-ID*	(Optional) Display the binding entry based on VLAN.
interface *INTERFACE-ID*	(Optional) Display the binding entry based on port ID.
,	(Optional) Specify a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specify a range of interfaces. No space before and after the hyphen.

Default Not applicable

Command Mode EXEC mode or any configuration mode

Usage Guideline Use the command to display DHCP snooping configuration binding entries.

Example This example shows how to display DHCP display DHCP snooping binding entries:

```
Switch# show ip dhcp snooping binding
Mac Address        IP Address      Lease(seconds)   Type          VLAN
Interface
----------------- --------------- -------------  -------------- ------ ----
-----
00-01-02-03-04-05 10.1.1.10       1500           dhcp-snooping   100
eth3.5
00-01-02-00-00-05 10.1.1.1        1495           dhcp-snooping   100
eth3.5

Total Entries: 2
Switch#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.1:

```
Switch# show ip dhcp snooping binding 10.1.1.1
Mac Address         IP Address      Lease(seconds)   Type           VLAN
Interface
----------------- --------------- -------------  -------------- ------ ----
-----
00-01-02-03-04-05 10.1.1.1         1500            dhcp-snooping   100
eth3.5

Total Entry: 1
Switch#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.11 and MAC 00-01-02-00-00-05:

```
Switch# show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05
Mac Address         IP Address      Lease(seconds)   Type           VLAN
Interface
----------------- --------------- -------------  -------------- ------ ----
-----
00-01-02-00-00-05 10.1.1.1         1495            dhcp-snooping   100
eth3.5

Total Entry: 1
Switch#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.1 and MAC 00-01-02-03-04-05 on vlan100:

```
Switch# show ip dhcp snooping binding 10.1.1.11 00-01-02-03-04-05 vlan 100
Mac Address       IP Address      Lease(seconds)   Type          VLAN
Interface
----------------- --------------- -------------  -------------- ------ ----
-----
00-01-02-03-04-05 10.1.1.1        1500           dhcp-snooping   100
eth3.5

Total Entry: 1
Switch#
```

This example shows how to display DHCP snooping binding entries by vlan100:

```
Switch# show ip dhcp snooping binding vlan 100
Mac Address       IP Address      Lease(seconds)   Type          VLAN
Interface
----------------- --------------- -------------  -------------- ------ ----
-----
00-01-02-03-04-05 10.1.1.10        1500           dhcp-snooping   100
eth3.5
00-01-02-00-00-05 10.1.1.11        1495           dhcp-snooping   100
eth3.5

Total Entries: 2
Switch#
```

This example shows how to display DHCP snooping binding entries by interface eth3.5:

```
Switch# show ip dhcp snooping binding interface eth3.5
Mac Address       IP Address      Lease (seconds)   Type          VLAN
Interface
----------------- --------------- -------------  -------------- ------ ----
-----
00-01-02-03-04-05 10.1.1.10        1500           dhcp-snooping   100
eth3.5
00-01-02-00-00-05 10.1.1.11        1495           dhcp-snooping   100
eth3.5

Total Entries: 2
Switch#
```

show ip dhcp snooping database

This command is used to display the statistics of the DHCP snooping database.

show ip dhcp snooping database

Syntax None

Default Not applicable

Command Mode EXEC mode or any configuration mode

Usage Guideline User can use this command to display DHCP snooping database statistics

Example This example shows how to display DHCP snooping database statistics:

```
Switch# show ip dhcp snooping database
Successful Transfer:     0     Failed Transfer  :     0
Binding Collisions :     0     Expired lease    :     0
Invalid interfaces :     0
Parse failures     :     0

Switch#
```

show erps domain

The show erps domain command is used to display information of all created ERPS domains.

show erps domain [*DOMAIN-NAME***]**

Syntax Description	
DOMAIN-NAME	Specifies the name of ERPS domain with a maximum of 32 characters. (Only allow character set: '0-9'. 'a-z', 'A-Z' '-')

Default Not applicable

Command Mode EXEC mode or any configuration mode

Usage Guideline This command displays brief instance information of all created ERP instances in an ERPS domain on a device.

Example The following example displays instance information of all created ERPS domains when ERPS is globally disabled:

```
Switch# show erps domain

ERPS is globally disabled

Switch#
```

The following example displays instance information of all created ERPS domains:

```
Switch# show erps domain

Domain                    ERPI  Type    Status         Port-State
  ID
--------------------- ---- ------ ---------- -------------------------
campus1                      1 Major   Idle           East:Blocked
                                                      West:Forwarding
campus1                      2 Sub     Protection     East:Virtual-Channel
                                                      West:Forwarding

campus2                      3 Major   Disabled       East: -
                                                      West: -

Total ERPS domains : 2
Total ERP instances : 3

Switch#
```

The following example displays instance information of ERPS domain campus1:

```
Switch# show erps domain campus1

Domain                    ERPI  Type    Status       Port-State
  ID
--------------------- ---- ------ ---------- -------------------------
campus1                      1 Major   Idle           East:Blocked
                                                      West:Forwarding
campus1                      2 Sub     Protection     East:Virtual Channel
                                                      West:Forwarding

Total ERP instances in domain campus1 : 2

Switch#
```

show erps erpi

The show erps erpi command is used to display information of ERP instance.

show erps erpi [*INSTANCE-ID***]**

Syntax

INSTANCE-ID	Specifies the identifier of ERP instance which will be showed. (Range: 1-4095)

Default Not applicable

Command Mode EXEC mode or any configuration mode

Usage Guideline The command "show erps erpi" is used to display detailed information of ERP instance with parameter "INSTANCE-ID", and it will also display sub-ring information for the sub ERP instance.

- For the enabled ERP instance, it will display "operational" value of parameters, but if the "operational" and "configured" values of parameters are different, it will display both values.
- And, for disabled ERP instance, it will only display "configured" values of parameters.

Example The following example displays detailed information ERP instance 1:

```
Switch# show erps erpi 1

ERPS global state : Enabled

ERP instance #1
-----------------------------------
Domain name : campus1
Instance type : Major
Instance state : Enabled
Instance status : Idle
R-APS controlled VLAN : 2
Ring MEL : 1
East ring port : eth3.1
East ring port state : Blocked
West ring port : eth3.2
West ring port state : Forwarding
RPL owner port : East
Service protected VLANs : 10-20
Guard timer : 500 milliseconds
Hold-Off timer : 0 milliseconds
WTR timer : 5 minutes

Switch#
```

The following example shows detailed information of sub ERP instance 2:

```
Switch# show erps erpi 2

ERPS global state : Enabled

ERP instance #2
-----------------------------------
Domain name : campus1
Instance type : Sub
Instance state : Disabled
Instance status : -
R-APS controlled VLAN : 3
Ring MEL : 1
East ring port : eth3.2[Shared]
East ring port state : -
West ring port : eth3.3
West ring port state : -
RPL owner port : (Not-configured)
Service protected VLANs : 15-25
Guard Timer : 500 milliseconds
Hold-Off Timer : 0 milliseconds
WTR Timer : 5 minutes

R-APS controlled virtual channel State : Enabled
R-APS controlled virtual channel VLAN : 3
Topology change propagation state : Enabled

Switch#
```

show vlan voice-vlan

Use this command to display the voice VLAN configurations.

show vlan voice-vlan [oui | interface INTERFACE-ID **[, | -]]**

show vlan voice-vlan [lldp-med] device [interface INTERFACE-ID **[, | -]]**

Syntax Description

oui	(Optional) Display OUI information of voice VLAN.
Interface	(Optional) Display voice VLAN information of ports.
INTERFACE-ID	(Optional) Specify the port to display.
,	(Optional) Specify a series of ports, or separate a range of ports from a previous range. No space before and after the comma.
-	(Optional) Specify a range of ports. No space before and after the hyphen.
lldp-med	(Optional) Display the voice devices that are discovered by LLDP-MED.
device	(Optional) Display the learned voice devices information.

Default None.

Command Mode EXEC mode or any configuration mode.

Usage Guideline This command is used to display the voice VLAN configurations and the information of learned voice devices.

Example This example displays the voice VLAN global settings.

```
Switch#show vlan voice-vlan

Voice VLAN Status     : Enabled
Voice VLAN ID          : 1000
CoS Priority           : 7
Aging time              : 60 minutes
Member ports           : eth3.1-3.5
Dynamic member ports : eth3.4

Switch#
```

This example displays the OUI information of voice VLAN.

```
Switch#show vlan voice-vlan oui

OUI Address         Mask                 Description
----------------    -----------------    -------------
00-01-e3-00-00-00   ff-ff-ff-00-00-00     Siemens
00-03-6b-00-00-00   ff-ff-ff-00-00-00     Cisco
00-09-6e-00-00-00   ff-ff-ff-00-00-00     Avaya
00-0f-e2-00-00-00   ff-ff-ff-00-00-00     Huawei&3COM
00-60-b9-00-00-00   ff-ff-ff-00-00-00     NEC&Philips
00-d0-1e-00-00-00   ff-ff-ff-00-00-00     Pingtel
00-e0-75-00-00-00   ff-ff-ff-00-00-00     Veritel
00-e0-bb-00-00-00   ff-ff-ff-00-00-00     3COM
01-02-03-04-05-06   ff-ff-ff-ff-ff-ff     UserDefined

Total Entries: 9

Switch#
```

This example displays the voice VLAN information of ports.

```
Switch#show vlan voice-vlan interface eth3.1-3.5

Interface       Status       Mode
-------------   ----------   --------
eth3.1          Enabled      Manual
eth3.2          Enabled      Manual
eth3.3          Enabled      Manual
eth3.4          Enabled      Manual
eth3.5          Enabled      Manual

Total Entries: 5

Switch#
```

This example displays the learned voice devices on ports eth3.1 and eth3.2.

```
Switch#show vlan voice-vlan device interface eth3.1-3.2

Interface      Voice Device Address
-------------  --------------------
eth3.1         00-03-6b-00-00-01
eth3.1         00-03-6b-00-00-02
eth3.1         00-03-6b-00-00-05
eth3.2         00-03-6b-00-00-09
eth3.2         00-03-6b-00-00-0a

Total Entries: 5

Switch#
```

This example displays the voice devices discovered by LLDP-MED. If the remaining time decreases to 0, the voice device will be deleted.

```
Switch#show vlan voice-vlan lldp-med device

Interface          : eth3.1
Chassis ID Subtype : MAC Address
Chassis ID         : 00-E0-BB-00-00-11
Port ID Subtype    : Network Address
Port ID            : 10.10.1.1
Create Time        : 10:09:05, 2011-05-20
Remain Time        : 120 Seconds

Interface          : eth3.5
Chassis ID Subtype : MAC Address
Chassis ID         : 00-E0-BB-00-00-12
Port ID Subtype    : Network Address
Port ID            : 10.10.1.2
Create Time        : 10:09:14, 2011-05-20
Remain Time        : 120 Seconds

Total Entries: 2

Switch#
```

show ip policy

Use the command to display the route map used for policy based routing.

show ip policy

Syntax Not applicable.

Default Not applicable.

Command Mode EXEC mode.

Usage Guideline The user can use the command to display the policy based routing configured on interfaces.

Example The following is sample output from the show ip policy command:

```
Switch#show ip policy

Interface       Route-map
------------ --------------------
vlan1           pbr-map1
Vlan2           pbr-map2
Vlan100         pbr-map3

Switch#
```

show ip arp inspection

Use this command to display the status of DAI for a specific range of VLANs.

show ip arp inspection [**interfaces** [*PORT* [, | -]] | **statistics** *VLAN* [, | -]]

Syntax

interfaces *PORT*	Specifies a port, range of ports or all ports to configure.
,	(Optional) Specify a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specify a range of interfaces. No space before and after the hyphen.
statistics *VLAN*	(Optional) Specified a VLAN or range of VLANs.

Default Not applicable

Command Mode EXEC mode or any configuration mode.

Usage Guideline If you do not enter the **statistics** keyword, the configuration and operating state of DAI for the selected range of VLANs is displayed. If you do not specify the interface name, the trust state for all applicable interfaces in the system are displayed.

Example This example shows how to display the statistics of packets that have been processed by DAI for VLAN 10:

```
Switch# show ip arp inspection statistics vlan 10
VLAN    Forwarded         Dropped    DHCP Drops
-----   ---------      -----------   ----------
   10         21546      145261     145261
VLAN    DHCP Permits      Source MAC Failures
-----   ------------      -------------------
   10         21546                        0
VLAN    Dest MAC Failures   IP Validation Failures
-----   -----------------   ----------------------
   10                   0                        0
Switch#
```

This example shows how to display the statistics of packets that have been processed by DAI for all active VLANs:

```
Switch# show ip arp inspection statistics
VLAN    Forwarded    Dropped    DHCP Drops
-----   ---------   ---------   ----------
    1           0           0            0
    2           0           0            0
   10       21546      145261       145261
  100           0           0            0
  200           0           0            0
 1024           0           0            0
VLAN    DHCP Permits      Source MAC Failures
-----   ------------      -------------------
    1              0                        0
    2              0                        0
   10          21546                        0
  100              0                        0
  200              0                        0
 1024              0                        0
VLAN    Dest MAC Failures   IP Validation Failures
-----   -----------------   ----------------------
    1                   0                        0
    2                   0                        0
   10                   0                        0
  100                   0                        0
  200                   0                        0
 1024                   0                        0
Switch#
```

This example shows how to display the configuration and operating state of DAI:

```
Switch# show ip arp inspection
Source MAC Validation     : Disabled
Destination Mac Validation: Disabled
IP Address Validation     : Disabled
VLAN    Configuration
-----   -------------
10      Enabled
Switch#
```

This example shows how to display the trust state of interface eth3.3:

```
Switch# show ip arp inspection interfaces eth3.3
Interface   Trust State
---------   -----------
eth3.3      untrusted
Switch#
```

This example shows how to display the trust state of interfaces on the switch:

```
Switch# show ip arp inspection interfaces
Interface   Trust State
---------   -----------
eth3.1      untrusted
eth3.2      untrusted
eth3.3      untrusted
eth3.5      Trusted
eth3.6      untrusted
eth3.7      untrusted
eth3.8      untrusted

Total Entries: 7
Switch#
```

show ip source binding

Use the command to display IP-source guard binding entry.

show ip source binding [*IP-ADDRESS*] [*MAC-ADDRESS*] **[dhcp-snooping | static] [vlan** *VLAN-ID***] [interface** *INTERFACE-ID* [, | -]]

Syntax

IP-ADDRESS	(Optional) Display the IP-source guard binding entry based on IP address.
MAC-ADDRESS	(Optional) Display the IP-source guard binding entry based on MAC address.
dhcp-snooping	(Optional) Display IP-source guard binding entry learned by DHCP binding snooping.
static	(Optional) Display IP-source guard binding entry that is manually configured.
vlan *VLAN-ID*	(Optional) Display the IP-source guard binding entry based on VLAN.
INTERFACE-ID	(Optional)Display the IP-source guard binding entry based on ports.
,	(Optional) Specify a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specify a range of interfaces. No space before and after the hyphen.

Default Not applicable

Command Mode EXEC mode or any configuration mode

Usage Guideline IP source guard use binding entries that are either manually configured or auto learned by DHCP snooping.

The command accepts combination of input options to filter the displayed entry.

Example This example shows how to display IP Source Guard binding entries without any parameter.

```
Switch# show ip source binding
MAC Address       IP Address      Lease(sec)  Type          VLAN   Interface
----------------- --------------- ---------- ------------- ----- ----------
------
00-01-01-01-01-01 10.1.1.10        infinite  static        100    eth3.3
00-01-01-01-01-10 10.1.1.11          3120    dhcp-snooping 100    eth3.3

Total Entries: 2
Switch#
```

This example shows how to display IP Source Guard binding entries by IP address 10.1.1.11.

```
Switch# show ip source binding 10.1.1.11
MAC Address       IP Address      Lease(sec)  Type          VLAN   Interface
----------------- --------------- ---------- ------------- ----- ----------
------
00-01-01-01-01-01 10.1.1.11        infinite  static        100    eth3.3

Total Entry: 1
Switch#
```

This example shows how to display IP Source Guard binding entries by IP address 10.1.1.11, MAC address 00-01-01-01-01-10 at VLAN100 on interface eth3.3 and learning by DHCP snooping:

```
Switch# show ip source binding 10.1.1.11 00-01-01-01-01-10 dhcp-snooping
vlan 100 interface eth3.3
MAC Address       IP Address      Lease(sec)  Type          VLAN   Interface
----------------- --------------- ---------- ------------- ----- ----------
------
00-01-01-01-01-10 10.1.1.11          3564    dhcp-snooping 100    eth3.3

Total Entry: 1
Switch#
```

show ip verify source

Use this command to display the port ACL entry on a particular interface.

show ip verify source [interface *INTERFACE-ID* [, | -]]

Syntax

INTERFACE-ID	Specifies a port or a range of ports to configure.
,	(Optional) Specify a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specify a range of interfaces. No space before and after the hyphen.

Default Not applicable

Command Mode EXEC mode or any configuration mode

Usage Guideline Use the command to display the port ACL entries for a port.

Example This example shows the display when the interface has an IP source filter mode that is configured as IP-MAC and an existing IP MAC binds 10.1.1.10 MAC address 00-01-01-01-01-01 on VLAN 100 and 10.1.1.11 MAC address 00-01-01-01-01-10 on VLAN 101:

```
Switch# show ip verify source interface eth3.3
Interface  Filter-type  Filter-mode  IP address       MAC address       VLAN
---------  -----------  -----------  ---------------  ----------------- ---
----
eth3.3       ip-mac     Active       10.1.1.10        00-01-01-01-01-01 100
eth3.3       ip-mac     Active       10.1.1.11        00-01-01-01-01-10 101
eth3.3       ip-mac     Active       deny-all         deny-all

Total Entries: 3
Switch#
```

show ip dhcp screening

Used to display the configuration of DHCP server screening

show ip dhcp screening

Syntax None.

Default Not applicable

Command Mode EXEC mode or any other configuration mode

Usage Guideline This command is used to display the configuration of DHCP server screening.

Example The following example shows the configuration which enables functions on port range from eth4.1 to eth4.23 and adds a binding composed of server IP 10.1.1.1 and client MAC address 00-08-01-02-03-04 on port from eth4.1 to 4.23:

```
switch# show ip dhcp screening

   Enable ports: eth4.1-4.23

   Filter DHCP Server Trap_Log State: Disabled
   Illegal Server Log Suppress Duration:1 minutes
   Filter DHCP Server/Client List:
      Server IP Address Client MAC Address Port
      10.1.1.1          00:08:01:02:03:04  eth4.1-4.23

   Total Entries: 1
```

show sflow

Use the **show sflow** command to display the sFlow information.

show sflow [agent|receiver|sampler|poller]

Syntax

agent	(Optional) Display the sFlow agent information.
receiver	(Optional) Display the information of all Receivers.
sampler	(Optional) Display the information of all Samplers.
poller	(Optional) Display the information of all Pollers.

Default None

Command Mode EXEC mode or any configuration mode.

Usage Guideline The keyword **[agent|receiver|sampler|poller]** indicates which type of sFlow object's information to be displayed. The show sflow command without keyword displays all types of sFlow objects' information.

Example This example shows how to display all types of sFlow objects' information. The flow samples and counter samples of eth3.1 are sent to 10.1.1.2. The flow samples and counter samples of eth3.2 are sent to both 10.1.1.2 and 10.1.1.3:

```
switch(config)# show sflow

sFlow Agent Version: 1.3;D-Link Corporation;2.00
sFlow Agent Address: 10.1.1.1
sFlow State        : Enabled

Receivers Information
Index                  : 1
Owner                  : collector1
Current Countdown Time: 86122
Max Datagram Size      : 1400
Address                : 10.1.1.2
```

```
Port                    : 6343
Datagram Version        : 5

Index                   : 2
Owner                   : collector2
Current Countdown Time: 86355
Max Datagram Size       : 1400
Address                 : 10.1.1.3
Port                    : 6343
Datagram Version        : 5

Index                   : 3
Owner                   : (NULL)
Current Countdown Time: 0
Max Datagram Size       : 1400
Address                 : 0.0.0.0
Port                    : 6343
Datagram Version        : 5

Index                   : 4
Owner                   : (NULL)
Current Countdown Time: 0
Max Datagram Size       : 1400
Address                 : 0.0.0.0
Port                    : 6343
Datagram Version        : 5
Samplers Information
 Interface   Instance   Receiver  Sampling Rate   Max Header Size
---------- --------- --------- -------------  --------------------
  eth3.1        1         1           256               128
  eth3.2        1         1           256               128
  eth3.2        2         2           512               256

Pollers Information
 Interface   Instance   Receiver    Interval
---------- --------- ---------- ------------
  eth3.1       1          1              10
  eth3.2       1          1              10
  eth3.2       2          2              20
```

show lldp

To displays the switch's general LLDP configuration, use the **show lldp** command.

show lldp

Syntax This command has no arguments or keywords.

Default Not applicable.

Command Mode EXEC mode or any configuration mode

Usage Guideline This command is used to show LLDP system global configurations.

Example This example shows how to display the LLDP system global configuration status:

```
Switch> show lldp
LLDP System Information
Chassis ID Subtype             : MAC Address
Chassis ID                     : 00-33-50-43-00-00
System Name                    : Switch
System Description             : Stackable Ethernet Switch
System Capabilities Supported : Bridge, Router
System Capabilities Enabled    : Bridge, Router

LLDP-MED System Information
Device Class                   : Network Connectivity Device
Hardware Revision              : 0A
Firmware Revision              : XXXXXXXXXX
Software Revision              : XXXXXXXXXX
Serial Number                  : 123456789-123456789-123456789-01
Manufacturer Name              : D-Link Corporation.
Model Name                     : DGS-6604
Asset ID                       : XXXXXXXXXX
PoE Device Type                : PSE Device
PoE PSE Power Source           : Primary
LLDP Configuration
LLDP State                    : Disabled
Message Tx Interval            : 30
Message Tx Hold Multiplier     : 4
Reinit Delay                   : 2
Tx Delay                       : 2

LLDP-MED Configuration
Fast Start Repeat Count        : 4

Switch>
```

show lldp interface

To display the LLDP each physical interface configuration for advertisement options, use the **show lldp interface** command in user EXEC mode.

show lldp interface INTERFACE-ID [, | -]

Syntax Description

INTERFACE-ID	Displays LLDP configuration for a specific interface. Valid interfaces are physical interface.
,	(Optional) Specifies a series of physical interfaces. No space before and after the comma.
-	(Optional) Specifies a range of physical interfaces. No space before and after the hyphen.

Default Not applicable

Command Mode EXEC mode or any configuration mode

Usage Guideline This command displays the LLDP each physical interface configuration for advertisement options.

Examples The following is sample output from the show lldp interface command. To display a specific physical interface configuration:

```
Switch> show lldp interface eth4.4

Port ID: eth4.4
Port ID                                 : eth4.4
Admin Status                            : TX and RX
Basic Management TLVs:
    Port Description                    : Disabled
    System Name                         : Disabled
    System Description                  : Disabled
    System Capabilities                 : Disabled
    Enabled Management Address          :
        IPv4 Address:
          192.168.254.10, 192.168.254.11
        IPv6 Address:
          3ffe:501:ffff:100:a01:2ff:fe39:1,
          FE80::250:A2FF:FEBF:A056
IEEE 802.1 Organizationally Specific TLVs:
    Port VLAN ID                        : Disabled
    Enabled Port and Protocol VLAN ID :
        6,7
    Enabled VLAN Name                   :
        1-5, 8-10
    Enabled Protocol Identity           :
        EAPOL, GVRP

IEEE 802.3 Organizationally Specific TLVs:
    MAC/PHY Configuration/Status        : Disabled
    Power Via MDI                       : Disabled
    Link Aggregation                    : Disabled
    Maximum Frame Size                  : Disabled
LLDP-MED Organizationally Specific TLVs:
    Capabilities TLV                    : Disabled
    Network Policy TLV                  : Disabled
    Extended Power Via MDI PSE TLV      : Disabled
    Inventory TLV                       : Disabled

Switch>
```

show lldp local interface

To display the each physical interface information, which will be carried in the LLDP TLVs and sent to neighbor devices, use the show **lldp local interface** command.

show lldp local interface *INTERFACE-ID* **[, | -] [brief | detail]**

Syntax
Description

INTERFACE-ID	Display the currently available information to advertise LLDP for specific interface. Valid interfaces are physical interface
,	(Optional) Specify a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specify a range of interfaces. No space before and after the hyphen.
brief	(Optional) Display the information in brief mode.
detail	(Optional) Display the information in detailed mode.
	If neither **brief** nor **detail** is specified, display the information in normal mode.

Default Not applicable

Command Mode EXEC mode or any configuration mode

Usage Guideline This command displays the each physical interface information currently available for populating outbound LLDP advertisements. If the advertising TLVs are classified as global information, e.g. System Name, use the command **show lldp** to get them.

Example The following is sample output from the show lldp local interface command to display outbound LLDP advertisements for eth4.4 in detailed mode.:

```
Switch> show lldp local interface eth4.4 detail

Port ID : eth4.4
------------------------------------------------------------------------------
--
Port ID Subtype                              : MAC Address
Port ID                                      : 08-03-04-17-00-03
Port Description                             : RMON Port 4 on Unit 4
Port VLAN ID                                 : 1
Management Address Count                     : 2
    Subtype                                  : IPv4
    Address                                  : 10.1.1.1
    IF Type                                  : IfIndex
    OID                                      : 1.3.6.1.4.1.171.10.36.1.11
    Subtype                                  : IPv6
    Address                                  : FE80::250:A2FF:FEBF:A056
    IF Type                                  : IfIndex
    OID                                      : 1.3.6.1.4.1.171.10.36.1.11

PPVID Entries Count                          : 2
    Entry 1 :
        Port and Protocol VLAN ID            : 4
        PPVID Supported                      : Supported
        PPVID Enable                         : Enabled

    Entry 2 :
        Port and Protocol VLAN ID            : 5
        PPVID Supported                      : Supported
        PPVID Enable                         : Enabled

VLAN Name Entries Count                      : 1
    Entry 1 :
        VLAN ID                              : 1
        VLAN Name                            : VLAN0001
```

```
Protocol Identity Entries Count              : 1
    Entry 1 :
        Protocol Index                       : 4
        Protocol ID                          : 00 27 42 42 03 00 00 03
        Protocol Name                        : STP


MAC/PHY Configuration/Status                 :
    Auto-Negotiation Support                 : Supported
    Auto-Negotiation Enabled                 : Enabled
    Auto-Negotiation Advertised Capability   : 6c03(hex)
    Auto-Negotiation Operational MAU Type    : 0000(hex)

Power Via MDI                                :
   Port Class                                : PES
   PSE MDI Power Support                     : Supported
   PSE MDI Power State                       : Enable
   PSE Pairs Control Ability                 : Uncontrollable
   PSE Power Pair                            : 0
   Power Class                               : 2

Link Aggregation                             : Supported
    Aggregation Capability                   : Aggregated
    Aggregation Status                       : Not Currently in Aggregation
    Aggregation Port ID                      : 0

Maximum Frame Size                           : 1536

LLDP-MED Capabilities Support                :
    Capabilities                             : Support
    Network Policy                           : Support
    Location Identification                  : Not Support
    Extended Power Via MDI PSE               : Support
    Extended Power Via MDI PD                : Not Support
```

```
    Inventory                                 : Support

Network Policy                                :
  Application type                            : Voice
  VLAN ID                                     :  100
  Priority                                    :  7
  DSCP                                        :  0
  Unknown                                     :  False
  Tagged                                      :  True

Extended Power-Via-MDI TLV                    :
   Power priority                             :   High
   Power value                                :   30 Watts
Switch>
```

The following is sample output from the show lldp local interface command to display outbound LLDP advertisements for eth3.1 in brief mode.

```
Switch> show local interface eth3.1 brief
Port ID : eth3.1
------------------------------------------------------------------------
Port ID Subtype               : MAC Address
Port ID                       : 06-48-D0-11-00-17
Port Description              : RMON Port 1 on Unit 1

Switch>
```

```
Switch> show lldp local interface eth 3.1
Port ID : eth3.1
------------------------------------------------------------------------
Port ID Subtype                 : MAC Address
Port ID                         : 08-03-04-17-00-03
Port Description                : RMON Port 1 on Unit 3
Port VLAN ID                    : 1
Management Address Count        : 2
PPVID Entries Count             : 3
VLAN Name Entries Count         : 3
Protocol Identity Entries Count: 2
MAC/PHY Configuration Status    : (See Detail)
Link Aggregation                : (See Detail)
Maximum Frame Sixe              : 1000

LLDP-MED capabilities           : (See Detail)
Extended Poer via MDI           : (See Detail)
Network policy                  : (See Detail)

Switch>
```

show lldp management-address

To display the LLDP management address information, use the show lldp management-address in user EXEC mode.

show lldp management-address [IP-ADDRESS | IPV6-ADDRESS **]**

Syntax Description	
IP-ADDRESS	(Optional) Display the LLDP management information for specific IPv4 address.
IPV6-ADDRESS	(Optional) Display the LLDP management information for specific IPv6 address.

Default Not applicable

Command Mode EXEC mode or any configuration mode

Usage Guideline **show lldp management-address** is issued without arguments, all configured LLDP management address(es) will be displayed.

Example The following is sample output from the **show lldp management-address** command to display the LLDP management address information for 192.168.254.10:

```
Switch> show lldp management-address 192.168.254.10
Address 1:
------------------------------------------------------------------------
Subtype : IPv4
Address : 192.168.254.10
IF type  : IfIndex
OID  : 1.3.6.1.4.1.171.10.36.1.11
Advertising Ports  :
eth3.1-3.5, eth3.7, eth4.10-4.20
Switch>
```

This example shows how to display all management address information:

```
Switch> show lldp management-address
Address 1: (default)
-----------------------------------------------
  Subtype                           : IPv4
  Address                           : 10.90.90.90
  IF Type                           : IfIndex
  OID                               : 1.3.6.1.4.1.171.10.118.3
  Advertising Ports                 :
    eth3.1-3.3
Address 2 :
-----------------------------------------------
Subtype                             : IPv4
  Address                           : 10.90.90.90
  IF Type                           : IfIndex
  OID                               : 1.3.6.1.4.1.171.10.118.3
  Advertising Ports                 :
    eth3.4
Address 3 :
-----------------------------------------------
  Subtype                           : IPv4
  Address                           : 172.18.1.1
  IF Type                           : IfIndex
  OID                               : 1.3.6.1.4.1.171.10.118.3
  Advertising Ports                 : -

Address 4: (default)
-----------------------------------------------
  Subtype                           : IPv6
  Address                           : ::
  IF Type                           : IfIndex
  OID                               : 1.3.6.1.4.1.171.10.118.3
  Advertising Ports                 :
eth3.6
Total Entries : 4

Switch>
```

show lldp neighbor interface

To display the each physical interface information currently learned from the neighbor, use the s**how lldp neighbor interface** command.

show lldp neighbor interface *INTERFACE-ID* **[, | -] [brief | detail]**

Syntax Description

INTERFACE-ID	Valid interfaces are physical interface
,	(Optional) Specify a series of interfaces, or separate a range of interfaces from previous range. No space before and after the comma. from a previous range. No space before and after the comma.
-	(Optional) Specify a range of interfaces. No space before and after the hyphen.
brief	(Optional) Display the information in brief mode.
detail	(Optional) Display the information in detailed mode.

If neither **brief** nor **detail** is specified, display the information in normal mode.

Default Not applicable

Command Mode EXEC mode or any configuration mode

Usage Guideline This command display the information learned from the neighbor devices.

Example The following is sample output from the show **lldp neighbor interface** command to display information about neighboring devices learned by LLDP on eth4.9 in detailed mode:

```
Switch> show lldp neighbor interface eth4.9 detail

Port ID : eth4.9
------------------------------------------------------------------------
----
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                          : MAC Address
    Chassis ID                                  : 00-01-02-03-04-05
    Port ID Subtype                             : Local
    Port ID                                     : 1/5
    Port Description                            : RMON Port
    System Name                                 : Switch1
    System Description                          : Stackable Ethernet Switch
    System Capabilities Supported               : Repeater, Bridge
    System Capabilities Enabled                 : Repeater, Bridge
    Management Address Count                    : 0
        (None)

    Port VLAN ID                                : 0
    PPVID Entries Count                         : 0
        (None)

    VLAN Name Entries Count                     : 0
        (None)

    Protocol ID Entries Count                   : 0
        (None)

    MAC/PHY Configuration/Status                : (None)
    Power Via MDI                               : (None)
    Link Aggregation                            : (None)
    Maximum Frame Size                          : 0
    Unknown TLVs Count                          : 0
        (None)
```

```
LLDP-MED capabilities:
LLDP-MED device class                        : Endpoint device class III
       LLDP-MED capabilities support              :
           LLDP-MED capabilities                  : Support
           Network Policy                         : Support
           Location identification                : Not Support
           Extended power via MDI                 : Support
          Inventory                              : Support
      LLDP-MED capabilities enabled              :
          LLDP-MED capabilities                  : Enabled
          Network Policy                         : Enabled
          Location identification                : Enabled
          Extended power via MDI                 : Enabled
          Inventory                              : Enabled

  Extended power via MDI                         :
        Power device type                        : PD device
        Power source                             : from PSE
        Power request                            : 8 watts

  Network policy:
        Application type                         : Voice
        VLAN ID                                  : -
        Priority                                 : -
        DSCP                                     : -
        Unknown                                  : True
        Tagged                                   : -
        Extended power via MDI:
        Power device type: PD device
        Power Source: from PSE
        Power request: 8 watts
    Inventory Management                         : (None)
Switch>
```

The following is sample output from the show lldp neighbor interface eth3.1 command.

```
Switch> show lldp neighbor interface eth3.1
Port ID : 1
------------------------------------------------------------------------
Remote Entities Count : 2
Entity 1
Chassis ID Subtype             : MAC Address
Chassis ID                     : 00-01-02-03-04-01
Port ID Subtype                : Local
Port ID                        : eth3.1
Port Description               : RMON Port 3 on Unit 1
System Name                    : Switch1
System Description             : Stackable Ethernet Switch
System Capabilities Supported  : Repeater, Bridge
    System Capabilities Enabled : Repeater, Bridge
Management Address Count       : 1
Port VLAN ID                   : 1
PPVID Entries Count            : 5
VLAN Name Entries Count        : 3
Protocol ID Entries Count      : 2
MAC/PHY Configuration Status   : (See Detail)
Power Via MDI                  : (See Detail)
Link Aggregation               : (See Detail)
Maximum Frame Size             : 1536

LLDP-MED capabilities     : (See Detail)
Network policy                 : (See Detail)
Extended Power Via MDI          : (See Detail)
    Inventory Management    : (See Detail)
    Unknown TLVs Count             : 2
```

```
Entity 2
Chassis ID Subtype              : MAC Address
Chassis ID                      : 00-01-02-03-04-02
Port ID Subtype                 : Local
Port ID                         : 2/1
Port Description                : RMON Port 1 on Unit 2
System Name                     : Switch2
System Description              : Stackable Ethernet Switch
System Capabilities Supported             : Repeater, Bridge
System Capabilities Enabled : Repeater, Bridge
Management Address Count        : 2
Port VLAN ID                    : 1
PPVID Entries Count             : 5
VLAN Name Entries Count         : 3
Protocol Id Entries Count       : 2
MAC/PHY Configuration Status    : (See Detail)
Power Via MDI                   : (See Detail)
Link Aggregation                : (See Detail)
Maximum Frame Size              : 1536
    LLDP-MED capabilities     : (See Detail)
Extended power via MDI     : (See Detail)
Network policy                   : (See Detail)
    Inventory Management    : (See Detail)
Unknown TLVs Count              : 2

Switch>
```

The following is sample output from the show lldp neighbor interface command to display the neighbor information on eth3.1 to eth3.2 in brief mode.

```
Switch > show lldp neighbor interface eth3.1-3.2 brief
Port ID: eth3.1
------------------------------------------------------------
Remote Entities Count : 3
Entity 1
Chassis ID Subtype            : MAC Address
Chassis ID                    : 00-01-02-03-04-01
Port ID Subtype               : Local
Port ID                       : eth3.1
Port Description              : RMON Port 1 on Unit 3

Entity 2
Chassis ID Subtype            : MAC Address
Chassis ID                    : 00-01-02-03-04-02
Port ID Subtype               : Local
Port ID                       : eth1.4
Port Description              : RMON Port 1 on Unit 4

Port ID : eth3.2
------------------------------------------------------------------
Remote Entities Count : 3
Entity 1
Chassis ID Subtype            : MAC Address
Chassis ID                    : 00-01-02-03-04-03
Port ID Subtype               : Local
Port ID                       : eth2.1
Port Description              : RMON Port 2 on Unit 1

Entity 2
Chassis ID Subtype            : MAC Address
Chassis ID                    : 00-01-02-03-04-04
Port ID Subtype               : Local
Port ID                       : eth2.2
Port Description              : RMON Port 2 on Unit 2

Entity 3
Chassis ID Subtype            : MAC Address
Chassis ID                    : 00-01-02-03-04-05
Port ID Subtype               : Local
Port ID                       : eth3.2
Port Description              : RMON Port 2 on Unit 3

Switch>
```

show lldp statistics

To display the system global LLDP statistics information, use the show lldp statistics in user EXEC mode, use the show lldp statistics command.

show lldp statistics

Syntax This command has no arguments or keywords.

Default Not applicable

Command Mode EXEC mode or any configuration mode

Usage Guideline EXEC mode or any configuration mode

Example To display global statistics information:

```
Switch> show lldp statistics

Last Change Time  : 0DT0H2M24S
Total Inserts     : 1
Total Deletes     : 0
Total Drops       : 0
Total Ageouts     : 0
Interface PoE interface
```

show lldp statistics interface

To display the each physical interface LLDP statistics information, use the show lldp statistics interface command.

show lldp statistics interface INTERFACE-ID **[**, | -**]**

Syntax Description

INTERFACE-ID	Valid interfaces are physical interface
,	(Optional) Specify a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specify a range of interfaces. No space before and after the hyphen.

Default This command has no default settings.

Command Mode EXEC mode or any configuration mode

Usage Guideline The each physical interface LLDP statistics command displays each physical interface LLDP statistics.

Example To display statistics information of eth3.1:

```
Switch> show lldp statistics interface eth3.1
Port ID : eth3.1
------------------------------------------------------------------------
Total Transmits           : 27
Total Discards            : 0
Total Errors              : 0
Total Receives            : 27
Total TLV Discards        : 0
Total TLV Unknows         : 0
Total Ageouts             : 0

Switch>
```

show poe power system

Use the command to display the setting and actual values of the whole POE system.

show poe power system [unit UNIT-ID **[,-]] {power-info | parameters}**

Syntax Description

unit *UNIT-ID*	(Optional) Specify the unit to be displayed. If no specified unit, all supported PoE units are displayed. The value range of *UNIT-ID* is between 3 o 6.
, -	(Optional)You can specify a range of *UNIT-ID* by a hyphen, or a series of *UNIT-ID* by comma. There is no space before and after comma or hyphen.
power-info	This option could display the power information such as allocated power、used power and unit priority of specific PoE unit.
parameters	This option could display the parameters such as max ports、device ID、SW version、EEPROM status and configuration status for the PoE sub-system.

Default None

Command Mode EXEC mode or any configuration mode

Usage Guideline This command could display the detail power information and PoE chip parameters for each PoE capable unit. As list of an UNIT-ID list is specified and not all of units in the list are PoE capable, only the PoE capable units are displayed.

The delim sign for specifying unit list supports two choices: hyphen (-) or comma (,). The hyphen sign is used for displaying continuous units such as unit 2 to unit 4, and the format of the list will be "2-4". If you just want to check some units specifically like unit 3 and unit 4 which is not continuously arranged, and the comma sign can be used.

Example This example shows how to display PoE power system's power information.

```
Switch# show poe power system power-info
PoE system power budget: 2400 Watts(Total)
PoE system notification: enabled
PoE system service policy: preemptive
unit priority allocated(W) consumed(W) remaining(W)
-------------------------------------------
2    1st      750          740
3    2nd      630          115
4    3rd      120          14

-------------------------------------------
Total         1500         869        900
```

This example shows how to display the PoE system parameters with unit list contained of hyphen sign.

```
Switch# show poe power system unit 2-4 parameters
unit max ports device ID SW version EEPROM status       config status
---- --------- --------- ---------- -----------------  -------------
2      48          E101       4.0.1.2      0(update done)      1(dirty)
3      48          E101       4.0.1.2      0(update done)      0(saved)
4      48          E101       4.0.1.2      1(process update)   0(saved)
```

This example shows how to display the PoE system parameters with unit list contained of comma.

```
Switch# show poe power system unit 2,4 parameters
unit max ports device ID SW version EEPROM status       config status
---- --------- --------- ---------- -----------------  -------------
2      48          E101       4.0.1.2     0(update done)      0(saved)
4      48          E101       4.0.1.2     1(process update)   0(saved)
```

show poe power-inline

Use the **show power inline** to display the Power over Ethernet (PoE) status for the specified PoE port, or for all PoE ports in the switch system.

show poe power inline [INTERFACE-ID **] {status | statistic | measurement | description}**

Syntax Description

INTERFACE-ID	(Optional) Specify the interface to be displayed. The format of *INTERFACE-ID* is “ethx.x” for the single one and “ethx.x-y.y” for the interface range. If no specified interface, all supported PoE interfaces are displayed.
status	Display the port configuration status
statistic	Display the port error counters
measurement	Display the port voltage、current、consumed power and temperature
description	Display the port description string

Default None

Command Mode EXEC mode or any configuration mode

Usage Guideline The **show poe power-inline** command is used to display the PoE power inline configuration status ‘statistic counter’ measurement result and the port description string. If *INTERFACE-ID* is not specified with this command, then all of PoE interfaces will be shown. As list of an I*NTERFACE-ID* list is specified and not all of ports in the list are PoE capable, only the PoE capable interfaces are displayed.

If there is a non-PoE capable port listed in the I*NTERFACE-ID*, a warning message will be displayed to indicate this situation

Example This is an example of output from the **show poe power-inline status** command.

```
switch# show poe power inline status
Interface Priority PSE State       OP Mode Class    Max(mW) Used(W) Time-
Range
=============================================================================
====
3.1       1st      on  delivering  auto    class-1  4000    3.5     --
3.2       1st      on  delivering  auto    class-2  7000    6.7     rdtime
...
4.1       1st      on  delivering  static  class-3  15400   15.0     --
4.2*      1st      on  delivering  auto    class-3  15400   12.4     --
4.3       2nd     off searching   never   class-0  15400   0         daytime
4.4       2nd      off searching   static  class-0  11000   0          --
...
```

This is an example of output from the show poe power-inline statistic command.

```
switch# show poe power inline statistic
Interface MPS-Absent Overload Short Power-Denied Invalid-Signature
--------- ---------- -------- ----- ------------ -----------------
3.1       2          5        0     10           0
3.2       2          1        0      3           0
...
4.1       2          0        0      2           0
4.2       2          0        0      1           0
4.3       2          0        0      5           0
4.4       2          0        0      0           0
...
```

This is an example of output from the **show poe power-inline** measurement command.

```
switch# show poe power inline measurement
Interface Voltage(V) Current(mA) Temp(C)    Power(W)
--------- ---------- ----------- --------  --------
3.1       54.2       109.2       35         5.9
3.2       55         196.1       38        10.8
...
4.1       54.6       197.7       32        10.7
4.2       54.8       286.2       36        15.7
4.3       n/a        n/a         n/a       n/a
4.4       n/a        n/a         n/a       n/a
...
```

ssh

To start an encrypted session with a remote networking device, use the **ssh** command in user EXEC mode.

ssh [-c {**3des | aes128-cbc | aes256-cbc**}**] [-m** {**hmac-md5 | hmac-sha1 | hmac-sha1-96**}**] [-p** *PORT-NUMBER***] -l** *USERNAME* **{***IP-ADDRESS* | *IPV6-ADDRESS*}

Syntax

-c {3des | aes128-cbc | aes256-cbc}	(Optional)Specifies the crypto algorithm, 3DES, AES128-CBC or AES256-CBC, to use for encrypting data. If you do not specify the -c keyword, during negotiation the remote networking device sends all the supported crypto algorithms.
-m {hmac-md5 | hmac-sha1 | hmac-sha1-96}	(Optional)Specifies a Hashed Message Authentication Code (HMAC) algorithm, HMAC-MD5, HMAC-SHA1 or HMAC-SHA1-96. If you do not specify the -m keyword, during negotiation the remote networking device sends all the supported crypto algorithms.
-p *PORT-NUMBER*	(Optional) The TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the SSH protocol is 22.
-l *USERNAME*	Specifies the *USERNAME* to use when logging in as on the remote networking device running the SSH server.
IP-ADDRESS	IPv4 address of the host.
IPV6-ADDRESS	IPv6 address of the host.

Default None

Command Mode Management interface mode or User EXEC mode.

Usage Guideline The **ssh** command enables a device to make a secure, encrypted connection to another device running an SSH Version 2 server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

ssh command is allowed under both management interface mode and User EXEC mode. For User EXEC mode, the outgoing physical interfaces does not include management interface. If you are going to use ssh to login a device which can be reached only via the management port, you should use **ssh** command under management interface mode by entering **mgmt-if** command first.

Example The following example shows how to ssh to the ip address 20.74.19.200 with default port 22 (optional port parameter is provided). The ip address of 20.74.19.200 is management interface which allows user to long in.

```
Switch# ssh -l admin 20.74.19.200
admin@20.74.19.200's password:
 Chassis-based High-Speed Switch
                              Command Line Interface

                               Firmware: 1.50.B013
          Copyright (c) 2007 D-Link Corporation. All rights reserved.

Switch#
```

The following example shows a ssh session using the crypto algorithm aes128-cbc and an HMAC of hmac-sha1-96. The username is admin, and the IP is 20.74.19.200.

```
Switch# ssh -c aes128-cbc -m hmac-sha1-96 -l admin 20.74.19.200
admin@20.74.19.200's password:
 Chassis-based High-Speed Switch
                              Command Line Interface

                               Firmware: 1.50.B013
          Copyright (c) 2007 D-Link Corporation. All rights reserved.

Switch#
```

switchport voice-vlan state

Use the command to configure the voice VLAN state of ports.

switchport voice-vlan state {enable | disable}

Syntax Description

enable	Enable the voice VLAN function on ports.
disable	Disable the voice VLAN function on ports.

Default The default state is disabled.

Command Mode Interface configuration mode.

Usage Guideline This command is used to enable/disable the voice VLAN function on ports.

The command is available for physical port and port-channel interface configuration.

Example This example shows how to enable voice VLAN function on physical port eth3.1.

```
Switch(config)#interface eth3.1
Switch(config-if)#switchport voice-vlan state enable
Switch(config-if)#end
Switch#
```

You can verify your settings by entering **show vlan voice-vlan interface** command.

snmp-server

To enable the Simple Network Management Protocol (SNMP) agent, use the **snmp-server** command. To disable the SNMP agent, use the no form of this command.

snmp-server

no snmp-server

Syntax None

Default Disabled

Command Mode Global configuration

Usage Guideline The remote SNMP manager sends SNMP requests to agents and receives SNMP responses and notifications from agents. When the SNMP agent is enabled, the remote SNMP manager can query SNMP agents and send SNMP traps.

Examples This example shows how to enable the SNMP server.

```
Switch(config)# snmp-server
```

This example shows how to disable the SNMP server.

```
Switch(config)# no snmp-server
```

Verify the settings by entering the **show snmp-server** command.

snmp-server community

Use this command to set up the community access string to provide access to SNMP. Use the no form of the command to remove the specified community string.

snmp-server community *COMMUNITY-STRING* **[view** *VIEW-NAME* **] [ro | rw]**

no snmp-server community *COMMUNITY-STRING*

Syntax Description	
COMMUNITY-STRING	Defines the community string that consists of from 1 to 32 characters and functions much like a password, permiting access to the SNMP protocol. The syntax can use alphanumeric and special characters, but that does not allow space and '#' character.
view *VIEW-NAME*	(Optional) Name of a previously defined view. The view defines the objects available to the SNMP community.
ro	(Optional) Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
rw	(Optional) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default

There are two communities set in the default as shown below:

Community	View Name	Access right
private	CommunityView	Read/Write
public	CommunityView	Read Only

ro/rw: is set as read only (ro) if no **[**ro|rw**]** option is specified.

Command Mode

Global configuration at privilege level 15

Usage Guideline

This command creates a community entry in the community table.

This command provides a more user-friendly method to create a community string for V1/V2 management.

If the view name specified by the command, does not exist (i.e it was not created prior), then a new view will be created.

A community string is unable to be deleted if it has been associated with a snmp-server host.

Examples

This example shows how to set the read/write community string to comaccess in the mib2 view.

```
Switch(config)# snmp-server view mib2 1.3.6.1.2.1 included
Switch(config)# snmp-server community comaccess view mib2 rw
```

This example shows how to remove the community comaccess.

```
Switch(config)# no snmp-server community comaccess
```

Verify the settings by entering the **show snmp community** command.

snmp-server contact

Use this command to configure the system's snmp contact information. Use the no form of this command to remove the configuration of system contact information.

snmp-server contact *TEXT*

no snmp-server contact

Syntax Description	
contact *TEXT*	String that describes the system contact information.The maximum length is 255 characters (please refer to RFC1213 for the maximum length in detail). The syntax is a general string that allows space.

Default None

Command Mode Global configuration

Usage Guideline Configures the system's snmp contact information on the switch.

Example This example shows how to set the system's snmp contact information as the string *MIS Department II.*

```
Switch(config)# snmp-server contact MIS Department II
```

Verify the settings by entering the **show snmp-server** command.

snmp-server enable traps

To enable all Simple Network Management Protocol (SNMP) notification types that are available on the switch, use the **snmp-server enable traps** command. To disable all available SNMP notifications, use the no form of this command.

snmp-server enable traps

no snmp-server enable traps

Syntax None

Default Disabled

Command Mode Global configuration

Usage Guideline SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the snmp-server host traps command.

To configure the router to send these SNMP notifications, enter at least one **snmp-server enable traps** command. When entering the command with no keywords, all notification types are enabled. When entering the command with a keyword, only the notification type related to that keyword is enabled - see “snmp-server enable traps snmp” on page 827. To enable multiple types of notifications, issue a **separate snmp-server enable traps** command for each notification type and notification option.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, configure at least one **snmp-server host** command.

Example This example shows how to enable the SNMP traps.

```
Switch(config)# snmp-server enable traps
Switch(config)#
```

snmp-server enable traps snmp

To enable the sending of RFC 1157 Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps snmp** command. Use the no form of this command to disable RFC 1157 SNMP notifications,.

snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]

no snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]

Syntax Description	
authentication	(Optional) Controls the sending of SNMP authentication failure notifications. An authenticationFailure(4) trap signifies that the sending device is the addressee of a protocol message, that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs for packets with an incorrect community string. For SNMPv3, authentication failure occurs for packets with an incorrect SHA/MD5 authentication key or for a packet that is outside of the authoritative SNMP engine's window (for example, falls outside of configured access lists or time ranges).
linkup	(Optional) Controls the sending of SNMP linkUp notifications. A linkup(3) trap signifies that the sending device recognizes that one of the communication links, represented in the agent's configuration, has come up.
linkdown	(Optional) Controls the sending of SNMP linkDown notifications. A linkDown(2) trap signifies that the sending device recognizes a failure in one of the communication links, represented in the agent's configuration.
coldstart	(Optional) Controls the sending of SNMP coldStart notifications. A coldStart(0) trap signifies that the sending device is reinitializing itself such that, the agent's configuration or the protocol entity implementation may be altered.
warmstart	(Optional) Controls the sending of SNMP warmStart notifications. A warmStart(1) trap signifies that the sending device is reinitializing itself such that, neither the agent configuration nor the protocol entity implementation is altered.

Default All SNMP notifications are enabled by default.When issuing this command with none of the optional keywords, all RFC 1157 SNMP notifications are enabled (or disabled, if using the no form).

Command Mode Global configuration

Usage Guideline When issuing this command with no keywords, all notification types are enabled. If the command is entered with a keyword, only the notification type related to that keyword is enabled.

The **snmp-server enable traps snmp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, configure at least one **snmp-server host** command. For a host to receive a notification controlled by this command, both the **snmp-server enable traps**

command and the **snmp-server host** command for that host must be set to enabled.

The **snmp-server enable traps snmp [linkup] [linkdown**] form of this command globally enables SNMP linkUp and linkDown traps. After enabling either of these traps globally, disable these traps on specific interfaces using the **no snmp trap link-status** command in interface configuration mode. Note that in the interface level, *linkUp* and *linkDown* traps are enabled by default. This indicated that it is not necessary to enable these notifications on a per-interface basis.

Examples

The following example shows how to enable the router to send all traps to the host 10.9.18.100

```
Switch(config)# snmp-server enable traps snmp
Switch(config)# snmp-server host 10.9.18.100
```

The following example shows how to enable the switch to send all trap notifications to the host 10.9.18.100 using the community string defined as *public*:

```
Switch(config)# snmp-server enable traps snmp
Switch(config)# snmp-server host 10.9.18.100 version 2c public
```

The following example shows the enabling all SNMP trap types, then the disabling of only the **linkUp** and **linkDown** trap:

```
Switch> enable
Switch# configure terminal
Switch(config)# snmp-server enable traps snmp
Swtich(config)# end
Switch# show running-config | include traps snmpsnmp-server enable traps
snmp authentication linkup linkdown coldstart warmstart
Switch# configure terminal
Switch(config)# no snmp-server enable traps snmp linkup linkdown
Swtich(config)# end
Switch# show running-config | include traps snmpsnmp-server enable traps
snmp authentication coldstart warmstart
```

This example shows how to enable the SNMP authentication traps.

```
Switch(config)# snmp-server enable traps snmp authentication
```

Verify the settings by entering the **show snmp-server traps** command.

snmp-server engineID local

Use this command to specify the SNMP engine ID on the switch. Use the no form of the command to remove a configured SNMP engine ID and return the engine ID setting to the original default value.

snmp-server engineID local *ENGINEID-STRING*

no snmp-server engineID local

Syntax Description	
ENGINEID-STRING	String length from 10 to 24 characters that identifies the engine ID.

Default

An SNMP engine ID is generated automatically but is not displayed or stored in the running configuration.

Command Mode

Global configuration

Usage Guideline

The SNMP engine ID is a unique string used to identify the switch for administration purposes.It is not necessary to specify an engine ID for the switch. For further details on the SNMP engine ID, see RFC 3411.

To specify a manually configured ID, note that it is not necessary to specify the entire 24-character engine ID if the ID specified contains trailing zeros. Specify only the portion of the Engine ID up until the point where only zeros remain in the value. For example, to configure an engine ID of 123456789A00000000000000, specify an snmp-server engineID local as 123456789A.

For a single SNMP engine system, changing the SNMP engine ID will overwrite the old SNMP local engine ID setting.

Display the default or configured engine ID by using the **show snmp engineID** command.

Note: If the SNMP engine ID is set to the default value then the no form of the command will fail when it is executed.

Example

This example shows how to configure the SNMP engine ID to 123456789A00000000000000.

```
Switch(config)# snmp-server engineID local 123456789A
```

Verify the settings by entering the **show snmp engineID** command.

snmp-server group

Use this command to configure a new SNMP group or a table that maps SNMP users to SNMP views. Use the no form of the command to remove a specified SNMP group.

snmp-server group *GROUP-NAME* **{v1 | v2c | v3 {auth | noauth | priv}} [read** *READ-VIEW* **] [write** *WRITE-VIEW* **] [notify** *NOTIFY-VIEW***]**

no snmp-server group *GROUP-NAME*

Syntax Description	
GROUP-NAME	Specifies the name of the group. The valid length for GROUP-NAME is 1 to 32 characters. The syntax is a general string that does not allow space.
v1	Specifies that SNMPv1 (the least secure of the possible SNMP security models) should be used for the group.
v2c	Specifies that SNMPv2c should be used for the group.
v3	Specifies that SNMPv3 should be used for the group. SMNPv3 is the most secure of the supported security models, as it allow explicit configuration of the authentication characteristics.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
read *READ-VIEW*	(Optional) Specifies a read view for the SNMP group. The read-view argument represents a string that is the name of the view that enables the display to show only the contents of the agent.
write *WRITE-VIEW*	(Optional) Specifies a write view for the SNMP group. The write-view argument represents a string that is the name of the view that enables data entry to configure the contents of the agent.
notify *NOTIFY-VIEW*	(Optional) Specifies a notify view for the SNMP group.The notify-view argument represents a string that is the name of the view that enables a trap to be specified.

Default The default settings of SNMP group are as shown below:

Group Name	Version	Security Level	Read View Name	Write View Name	Notify View Name
initial	SNMPv3	noauth	restricted	None	restricted
ReadGroup	SNMPv1	noauth	CommunityView	None	CommunityView
ReadGroup	SNMPv2c	noauth	CommunityView	None	CommunityView
WriteGroup	SNMPv1	noauth	CommunityView	CommunityView	CommunityView
WriteGroup	SNMPv2c	noauth	CommunityView	CommunityView	CommunityView

Command Mode Global configuration

Usage Guideline

An SNMP group defines the access method, the read view, the write view, and the notification view.

For the access method, it means that when the user who belongs to this group must use the version and access method (for V3) to access the SNMP agent.

For the read view, it means that the user who belongs to this group can only read objects that are part of this view. For the write view, it means that the user who belongs to this group can only write objects that are part of this view. Accessing objects that are not part of the view will generate error messages.

For the notification view, it means that the system will check whether the trap manager owns the view to the binding objects that are associated with the notification packet. If the trap manager does not own the notification view to the binding objects, then the notification will not be sent to a trap manager.

Examples

This example shows how to create the SNMP server group *public* with SNMP v3.

```
Switch# configure terminal
Switch(config)#snmp-server group public v3 noauth
Switch(config)#
```

This example shows how to remove the SNMP server group *public* from the configuration.

```
Switch# configure terminal
Switch(config)# no snmp-server group public
Switch(config)# end
```

This example shows how to set a MIB view called interfacesMibView and create a group called guestgroup to SNMPv3 authentication-read mode associated with the MIB view.

```
Switch(config)#snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)# snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)#
```

Verify the settings by entering the **show snmp group** command.

snmp-server host

Use the command to specify the recipient of a SNMP notification operation. Use the no command to remove the recipient.

snmp-server host { *IP-ADDRESS* **} [version { 1| 2c | 3 {auth | noauth | priv } }]** *WORD* **[vlan-interface]**

no snmp-server host { *IP-ADDRESS* **}**

Syntax Description	
IP-ADDRESS	Name, IPv4 or IPv6 address of the SNMP notification host.
version	Optional) Version of the SNMP used to send the traps. The default is 1. If you use the **version** keyword, one of the following keywords must be specified: • **1** —SNMPv1. This option is not available with informs. • **2c** —SNMPv2C. • **3** —SNMPv3. The most secure model, because it allows packet encryption with the **priv** keyword. One of the following three optional security level keywords can follow the **3** keyword: – **auth**— Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. – **noauth**—Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3. – **priv**—Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
WORD	Password-like community string is sent with the notification operation. If the version is 3, The *COMMUNITY-STRING* is used as the *UserName*. The community string that consists of from 1 to 32 characters. The syntax is general string that does not allow space.
vlan-interface	When input IP-ADDRESS is IPv6 link-local address, user must choose an existing vlan-interface to specify output interface for a destination.

Default No host entry exists.

If no version option is specified, the default version is 1.

Command Mode Global configuration at privilege level 15

Usage Guideline SNMP notifications are sent as trap packets. If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must create at least one recipient of a SNMP notification by **snmp-server host** command.

To create an SNMP host where the notification will be sent to, the user can specify the version of notification packet. For V1 and V2 SNMP, the notification

will be sent in trap protocol data unit (PDU). For V3 SNMP, the notification will be sent in the SNMPv2-TRAP-PDU with the SNMPv3 header.

If the user specifies to send the notification in V3 format, the user can further specify whether to perform authentication and encryption of the packet. The switch will use the community string specified for this command as the user name and look up in the user table to get the password for the authentication and encryption.

For both V1/V2 and V3 SNMP, the switch will find out the notification view for the group associated with this SNMP host. If the binding variables associated with this notification are out of this notification view, then this notification will not send to the host.

For V3 SNMP host, the argument of WORD refers to a user created by the "**snmp-server user**" command. For V1/V2 SNMP host, the community string can only be created by the "**snmp-server community**" command. If the host version is not specified, the default value (SNMP v1) will be adopted and the WORD option must be a community string. There will be an error message displayed if user inputs a user name as WORD option. To create an SNMP host, the community string (for user) must be created first. An error message will be generated to indicate if it is not created.

If the host version is diffrent from the group version defined for the host (from the access control list option in the command "**snmp-server group**"), it will fail because the bersion is not matched. If the community is created, the system will create V1/V2 group implicitly.

Example

This example shows how to set up the trap recipient as 163.10.50.126 by using version 3 with security level: **auth** (MD5 and/or SHA packet authentication) and the SNMPv3 user: authuser.

```
Switch(config)# snmp-server user authuser authgroup v3 auth md5 1234
Switch(config)# snmp-server host 163.10.50.126 version 3 auth authuser
```

This example shows how to set up the trap recipient for IPv6 link-local address as fe80::64:84:154 by using version 2 with security level. The community string: public and this link-local address will be specifies output the vlan-interface: vlan1.

```
Switch(config)# snmp-server host fe80::64:84:154 version 2c public vlan1
```

You can verify your settings by entering the **show snmp host** command.

snmp-server location

Use this command to configure the system location information. Use the **no snmp-server locatio**n command to set the system location information to empty.

snmp-server location *TEXT*

no snmp-server location

Syntax Description	
location *TEXT*	A string that describes the system location information.The maximum length is 128 characters (please refer to RFC1213 for the maximum length in detail). The syntax is a general string that allows spaces.

Default Not configured

Command Mode Global configuration with privilege level 15

Usage Guideline Configure the system location information on the switch.

Example This example shows how to set up the system location information with string HQ 15F.

```
Switch(config)# snmp-server location HQ 15F
```

Verify the settings by entering the **show snmp-server** command.

snmp-server user

Use this command to configure a new Simple Network Management Protocol (SNMP) user. Use the **no snmp-server user** command to remove a user.

snmp-server user *USER-NAME GROUP-NAME* **v3 [encrypted] [auth { md5 | sha }** *AUTH-PASSWORD* **[priv** *PRIV-PASSWORD* **]]**

no snmp-server user *USER-NAME*

Syntax Description	
USER-NAME	The name of the user on the host that connects to the agent. The valid length is 1 to 32 characters. The syntax is a general string that does not allow spaces.
GROUP-NAME	The name of the group to which the user belongs. The valid length is 1 to 32 characters. The syntax is a general string that does not allow spaces.
v3	Specifies that the SNMPv3 security model should be used. Allows the use of the encrypted and or auth keywords.
encrypted	(Optional) Specifies whether the password appears in encrypted format (a series of digits, masking the true characters of the string).
auth	(Optional) Specifies which authentication level should be used.
md5	The HMAC-MD5-96 authentication level.
sha	The HMAC-SHA-96 authentication level.
AUTH-PASSWORD	The password used for authentication. For ***plain-text*** form, the password can be from 1 to 64 characters. The syntax is a general string that does not allow spaces. According to authentication level, the authentication key will be gererated. For ***encrypted*** form, the length is fixed to 16 octets for MD5 or 20 octets for SHA. The format is hex value, such as aa:bb:cc:dd.
PRIV-PASSWORD	The password used for privacy. For plain-text form, the password can be from 1 to 64 characters. The syntax is a general string that does not allow spaces. According to the authentication level, the private key will be generated by this string. If keyword enceypted is specified, the private key is specified by user, the format is hex value, such as aa:bb:cc:dd and the length is16 octets.

Default There is one preconfigured user:

USER-NAME: initial

GROUP-NAME: initial

Command Mode Global configuration with privilege level 15

Usage Guideline

Use this command to create an SNMP user. The group to which this user belongs must be created first. If this user belongs to a V3 group and also specifies authentication or encryption, then the password used for authentication and encryption needs to be defined.

An snmp user is unable to be deleted if it has been associated with an snmp-server host. An error message will appear to indicate this case.

The snmp user will not be able to manage the device if a password should be present but it is not present.

No default values exist for authentication or privacy algorithms when the command is configured. Also, no default passwords exist. The minimum length for a password is one character, although it is recommended to use at least eight characters for security. If a password is forgotten, it cannot be recovered and it and will need to manually reconfigured. Either a plain-text password or a localized message digest 5 (MD5) digest can be specified.

When using a localized MD5 or SHA digest, the string can be specified instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hex values.

Examples

In the following example, the plain-text password "hb123" is configured for the user "abcd" in the SNMPv3 group "public".

```
Switch(config)# snmp-server user abcd public v3 auth md5 hb123
```

In the following example, the MD5 digest string is used instead of the plain text password.

```
Switch(config)# snmp-server user abcd public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

Verify the settings by entering the **show snmp user** command.

snmp-server view

Use this command to create or update a view entry for SNMP. And use the **no snmp-server view** command to remove a specified SNMP view entry.

snmp-server view *VIEW-NAME OID-TREE* **{ included | excluded }**

no snmp-server view *VIEW-NAME*

Syntax Description	
VIEW-NAME	Label for the view record that being updating or created. The name is used to reference the record. The valid length for VIEW-NAME is 1 to 32 characters. The syntax is a general string that does not allow space.
OID-TREE	Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4.
included	(Optional) Configures the OID (and subtree OIDs) specified in the OID-TREE argument to be included in the SNMP view.
excluded	(Optional) Configures the OID (and subtree OIDs) specified in OID-TREE argument to be explicitly excluded from the SNMP view.

Default There are two VIEWs set as shown below:

VIEW-NAME	OID-TREE	View Type
restricted	1.3.6.1.2.1.1	Included
restricted	1.3.6.1.2.1.11	Included
restricted	1.3.6.1.6.3.10.2.1	Included
restricted	1.3.6.1.6.3.11.2.1	Included
restricted	1.3.6.1.6.3.15.1.1	Included
CommunityView	1	Included
CommunityView	1.3.6.1.6.3	Excluded
CommunityView	1.3.6.1.6.3.1	Include

Command Mode Global configuration at privilege level 15

Usage Guideline Use this command to create a view for the MIB object trees.

The view needs to be specified when the snmp-server group command is used to define a user group.

Example This example shows how to create a view that includes all objects in the MIB-II subtree.

```
Switch(config)# snmp-server view mib2 1.3.6.1.2.1 included
```

This example shows how to set a MIB view to interfacesMibView.

```
Switch(config)#snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)#
```

This example shows how to set the access rights for a group called guestgroup to SNMPv3 authentication-read mode.

```
Switch(config)#snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)#
```

Verify the settings by entering the **show snmp view** command.

sntp server

Use this command to allow the system clock to be synchronized with the SNTP time server. To remove a server from the list of SNTP servers, use the no form of this command.

sntp server *IP-ADDRESS*

no sntp server [*IP-ADDRESS* **]**

Syntax Description	
IP-ADDRESS	IP address of the time server which provides the clock synchronization.

Default Not configured

Command Mode Global configuration

Usage Guideline When using **no sntp server** without any option, the Switch will delete all configured SNTP servers and synchronization with the SNTP server will be disabled.

SNTP is a compact, client-only version of the NTP. SNTP can only receive the time from NTP servers; it cannot be used to provide time services to other systems.

SNTP typically provides time within100 milliseconds of a precise time source, but it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic, although it can be configured with extended access lists to provide some protection.

Enter this command once for each NTP server.

The switch must be configured with this global configuration command in order to enable SNTP.

Create multiple SNTP servers by entering this command multiple times with different SNTP server IP addresses.

The time obtained from the SNTP server refers to the UTC time.

Example The following example shows how to configure a switch to allow its software clock to be synchronized with the clock by the SNTP server at IP address 192.168.22.44:

```
Switch# configure terminal
Switch(config)# sntp server 192.168.22.44
Switch(config)# end
```

Verify the settings by entering the **show sntp server** command.

spanning-tree (Global configuration)

Use this command to enable STP mode. Use the no form of the command to disable STP.

spanning-tree

no spanning-tree

Syntax None

Default Disable

Command Mode Global configuration

Usage Guideline When the **no spanning-tree** command is used globally to disable STP, an STP BPDU will be treated as a normal multicast packet and it will be flooded to the other VLAN member ports.

Example This example shows how to enable STP and MSTP mode as the default mode.

```
Switch(config)# spanning-tree
Switch(config)#
```

Verify the settings by entering the **show spanning-tree** command.

spanning-tree (Interface configuration)

This setting is used to configure the STP function on the specified port. Use the no form of the command to disable the function.

spanning-tree

no spanning-tree

Syntax None

Default Enabled

Command Mode Interface configuration

Usage Guideline When setting the interface with the **no spanning-tree** command, the interface will not participate in the spanning tree topology port state calculation.

If the global spanning-tree state is disabled (no matter STP is disabled/enabled at the interface), then STP BPDU is treated as a normal multicast packet and will be flooded to the other VLAN member ports.

If the global spanning-tree state is enabled, then the STP state at the interface must be enabled, then the interface can participate in the STP calculation.

Both physical ports and channel group are valid interfaces for this command.

Example This example shows how to configure the STP state for interface port eth3.7.

```
Switch(config)# interface eth3.7
Switch(config-if)# spanning-tree
```

Verify the settings by entering the **show spanning-tree interface** command.

spanning-tree (timers)

Use this command to set the value of Spanning-Tree Timers. It is only used for RSTP and STP version.

spanning-tree [hello-time *SECONDS* **| forward-time** *SECONDS* **| max-age** *SECONDS* **]**

Syntax Description	
hello-time *SECONDS*	Specifies the time interval to send one BPDU at the Designated Port. The range is 1 to 10 seconds.
forward-time *SECONDS*	Specify the maximum delay time for one BPDU to be transmitted by a bridge and received from another bridge. The range is 4 to 30 seconds.
max-age *SECONDS*	Specify the time interval to determine if a BPDU is valid. The range is 6 to 40 seconds

Default

hello-time:2

forward-time: 15

max-age: 20

Command Mode

Global configuration

Usage Guideline

There are some constraints on the relationship of the three timers. Please refer to the following formulas :

2 × (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 × (Bridge_Hello_Time + 1.0 seconds)

An error message will be returned if the equation is not satisfied.

This configuration will take effect on STP version and RSTP version only.In MSTP mode, Use the command **spanning-tree mst (timers)** to configure the MSTP timers.

Example

This example shows how to configure the STP timers.

```
Switch(config)# spanning-tree hello-time 1
Switch(config)# spanning-tree forward-time 16
Switch(config)# spanning-tree max-age 21
```

Verify the settings by entering the **show spanning-tree** command.

spanning-tree cost

This setting is used to configure the value of port path-cost on the specified port.

spanning-tree cost *COST*

no spanning-tree cost

Syntax Description	
COST	Specifies the path cost for the port. The range is 1 to 200000000.

Default The path cost is computed from the bandwidth setting of the interface.

Command Mode Interface configuration

Usage Guideline Both physical port and port-channel interfaces are valid for this command,.

In RSTP / STP-Compatible mode, the administrative path cost is used by the single spanning-tree when accumulating the path cost to reach the Root.

In MSTP mode, the administrative path cost is used by the CIST regional root when accumulating the path cost to reach the CIST root.

Example This example shows how to configure the port cost to 20000 for eth3.7.

```
Switch(config)#interface eth3.7
Switch(config-if)#spanning-tree cost 20000
```

Verify the settings by entering the **show spanning-tree interface** command.

spanning-tree fast-forwarding

To enable fast forwarding mode, use the **spanning-tree fast-forwarding** command. When fast forwarding is enabled the interface will be immediately put into the forwarding state upon linkup without waiting for the timer to expire.

spanning-tree fast-forwarding

no spanning-tree fast-forwarding

Syntax None

Default Default fast forwarding is automatically derived from an IEEE Std 802.1D-2004 Bridge Detection state machine.

Command Mode Interface configuration (physical and port-channel interfaces)

Usage Guideline Use this command only with interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data-packet loop and disrupt the switch and network operations.

During linkup, when an interface, with fast-forwading mode enabled, is moved directly to the spanning-tree forwarding state, then it is not necessary to wait for the standard forward-time delay.

This command has two states:

- *spanning-tree fast-forwarding* -This command enables fast forwarding state unconditionally on the given port.
- *no spanning-tree fast-forwarding* -The fast-forwarding state for the given port is returned to the default settings.

This configuration will take effect on all the spanning-tree modes.

Example This example shows how to configure the fast-forwarding state at eth3.7.

```
Switch(config)#interface eth3.7
Switch(config-if)#spanning-tree fast-forwarding
```

Verify the settings by entering the **show spanning-tree interface** command.

spanning-tree guard root

To enable the guard mode, use the **spanning-tree guard** command. To return to the default settings, use the no form of this command.

spanning-tree guard root

no spanning-tree guard

Syntax None

Default Disabled

Command Mode Interface configuration (physical port and port-channel interfaces)

Usage Guideline This feature is used in a service-provider environment where the network administrator needs to prevent a low speed port becoming a root port for the local bridge networks. This configuration will take effect on all the spanning-tree versions.

Example This example shows how to configure eth3.1 to prevent if from becoming a root port.

```
Switch(config)#interface eth3.1
Switch(config-if)# spanning-tree guard root
```

Verify the settings by entering the **show spanning-tree interface** command.

spanning-tree link-type

To configure a link type for a port, use the **spanning-tree link-type** command. To return to the default settings, use the no form of this command.

spanning-tree link-type { point-to-point | shared }

no spanning-tree link-type

Syntax Description	
point-to-point	Specifies that the port's link type is point-to-point.
shared	Specifies that the port's link type is a shared media connection.

Default Link type is automatically derived from the duplex setting unless the link-type is explicitly configured.

Command Mode Interface configuration (available for both physical port and port-channel)

Usage Guideline A full-duplex port is considered to have a point-to-point connection; whereas conversely, a half-duplex port is considered to have a shared connection. The port cannot transit into forwarding state rapidly by setting the link type to shared-media. Hence, auto-determination of the link-type by the STP module is recommended.

This configuration will take effect on all the spanning-tree modes.

Example This example shows how to configure the link type to point-to-point for eth3.7.

```
Switch(config)# interface eth3.7
Switch(config-if)# spanning-tree link-type point-to-point
```

Verify the settings by entering the **show spanning-tree interface** command.

spanning-tree mode

Use this command to decide the STP mode. To return to the default settings, use the no form of this command.

spanning-tree mode { mstp | rstp |stp }

no spanning-tree mode

Syntax Description	
mstp	Multiple Spanning Tree Protocol (MSTP).
rstp	Rapid Spanning Tree Protocol (RSTP).
stp	Spanning Tree Protocol (IEEE 802.1D-Compatible)

Default **mstp**

Command Mode Global configuration

Usage Guideline If the spanning-tree mode is configured as STP or RSTP, all currently running MSTP instances will be cancelled automatically.

If the newly configured spanning-tree mode is changed from the previous one, the spanning-tree state machine will restart again, therefore all of the stable spanning-tree port states will transit into discarding states.

Caution: Be careful when using the spanning-tree mode command to switch between STP, RSTP, and MSTP modes. When entering the command, all spanning-tree instances are stopped for the previous mode and are restarted in the new mode. Using this command may cause disruption of the user traffic.

Example This example shows how to configure the running version of STP module to RSTP.

```
Switch(config)# spanning-tree mode rstp
```

Verify the settings by entering the **show spanning-tree** command.

spanning-tree mst (cost | port-priority)

To set the path cost and port-priority parameters for any MST instance (including the CIST with instance ID 0), use the s**panning-tree mst** command. To return to the default settings, use the no form of this command.

spanning-tree mst *INSTANCE-ID* **{cost** *COST* **| port-priority** *PRIORITY***}**

no spanning-tree mst *INSTANCE-ID* **{cost | port-priority}**

Syntax Description	
INSTANCE-ID	MSTP instance identifier; valid values are from 0 to 63, the number of supported MSTP instances is project dependent. Instance 0 represents the default instance, CIST.
cost *COST*	(Optional) Path cost for an instance; valid values are from 1 to 200000000.
port-priority *PRIORITY*	(Optional) Port priority for an instance; valid values are from 0 to 240 in increments of 16.

Default

COST: depends on the port speed; a faster interface speeds indicate smaller costs. MST always uses long path costs.

PRIORITY: 128

Command Mode

Interface configuration

Usage Guideline

Higher *COST* cost values indicate higher costs. When entering the cost, do not include a comma in the entry; for example, enter 1000, not 1,000.

Smaller port-priority PRIORITY values indicate higher priorities.

Examples

This example shows how to set the interface path cost:.

```
Switch(config)#interface eht3.1
Switch(config-if)# spanning-tree mst 0 cost 17031970
```

This example shows how to set the interface path cost:

```
Switch(config)#interface portchannel1
Switch(config-if)# spanning-tree mst 0 port-priority 64
```

spanning-tree mst (forward | max-age | max-hops)

Use this command to configure the Protocol Timers used by the STP module in MSTP mode.

spanning-tree mst { forward-time *SECONDS* **| max-age** *SECONDS* **| max-hops** *HOP-COUNT* **}**

Syntax Description	
forward-time *SECONDS*	The maximum delay time in seconds for one BPDU to be transmitted by a bridge and received from another bridge. The range is 4 to 30 seconds.
max-age *SECONDS*	Used to determine if a BPDU is valid. The range is 6 to 40 seconds.
max-hops *HOP-COUNT*	Used to restrict the forwarded times of one BPDU. The range is 1 to 20 hops.

Default **forward-time**:15 seconds

max-age: 20 seconds

max-hops: 20 hops

Command Mode Global configuration

Usage Guideline There are some constraints on the relationship of the three timers. Please refer to the following formulas:

2 × (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 × (Bridge_Hello_Time + 1.0 seconds)

Example This example shows how to configure bridge timers for MSTP version.

```
Switch# configure terminal
Switch(config)#spanning-tree mst forward-time 14
Switch(config)#spanning-tree mst max-age 19
Switch(config)#spanning-tree mst max-hops 19
Switch(config)# end
```

spanning-tree mst configuration

To enter MST-configuration submode, use the **spanning-tree mst configuration** command. To return to the default settings, use the no form of this command.

spanning-tree mst configuration

no spanning-tree mst configuration

Syntax None

Default The default value for the MST configuration is the default value for all its parameters:

- No VLANs are mapped to any MST instance (all VLANs are mapped to the CIST instance).
- The region name is the Bridge MAC Address.

Command Mode Global configuration

Usage Guideline The MST configuration consists of three main parameters:

- Instance VLAN mapping-See the **instance** command
- Region name-See the **name** (MST configuration submode) command
- Configuration revision number-See the **revision** command

The **exit** command is used to leave MST configuration submode.

Changing an MST-configuration submode parameter can cause connectivity loss. To reduce service disruptions, when entering the MST-configuration submode, make changes first to a copy of the current MST configuration before applying them at the submode.

.Examples This example shows how to enter MST-configuration submode:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)#
```

This example shows how to reset the MST configuration to the default settings:

```
Switch(config)# no spanning-tree mst configuration
Switch(config)#
```

spanning-tree mst hello-time

Use this command to configure the per port hello time used in MSTP version.

spanning-tree mst hello-time *SECONDS*

Syntax Description	
SECONDS	Used to determine the time interval to send one BPDU at the Designated Port. The range is 1 to 10.

Default *SECONDS*: 2

Command Mode Interface configuration

Usage Guideline The MSTP hello-time is only referenced in MSTP mode.

Both physical ports and port-channel interfaces are valid for this command.

Example This example shows how to configure the port hello-time to 1 for eth3.1.

```
Switch(config)#interface eth3.1
Switch(config-if)#spanning-tree mst hello-time 1
```

Verify the settings by entering the **show spanning-tree mst interface** command.

spanning-tree mst priority

Use this command to configure the bridge priority value for the selected MSTP instance. Use the no form of the command to return the setting to the default setting.

spanning-tree mst *INSTANCE-ID* **priority** *PRIORITY*

no spanning-tree mst *INSTANCE-ID* **priority**

Syntax Description	
INSTANCE-ID	Specifies the MSTP instance identifier. Valid values are from 0 to 63. The number of supported MSTP instances is project dependent. Instance 0 represents the default instance, CIST.
PRIORITY	Specifies the bridge priority. The priority value must be divisible by 4096 and the range is from 0 to 61440.

Default *PRIORITY*: 32768

Command Mode Global configuration

Usage Guideline The number of supported MSTP instances is project dependent.

This priority has same definition as the “spanning-tree priority” on page 854 within the STP command set, but it can specify different priorities for each distinct MSTP instance.

Example This example shows how to configure bridge priority for the MSTP instance 2.

```
Switch# configure terminal
Switch(config)#spanning-tree mst 2 priority 0
Switch(config)# end
```

Verify the settings by entering the **show spanning-tree mst** command.

spanning-tree port-priority

This setting is used to configure the value of the STP port priority on a specified port. It is only used for RSTP and STP version. Use the no form of this command to reset to the default priority.

spanning-tree port-priority *PRIORITY*

no spanning-tree port-priority

Syntax Description	
PRIORITY	Specifies the port priority; valid values are from 0 to 240.

Default *PRIORITY*: 128

Command Mode Interface configuration

Usage Guideline The port priority and the port number together form the Port Identifier. It will be used in the computation of the port's role. This parameter is used only in RSTP / STP-Compatible mode only. The port priority value must be divisible by 16, and a lower priority value (number) represents a higher priority.

Both of the physical port or port-channel interfaces are valid interfaces for configuration.

An error message will be returned if the priority is not a valid value.

Example This example shows how to configure the port priority to 0 for eth3.7.

```
Switch(config)#interface eth3.7
Switch(config-if)#spanning-tree port-priority 0
```

Verify the settings by entering the **show spanning-tree interface** command.

spanning-tree priority

This command configures the bridge priority and is only used for RSTP and STP versions. Use the no form of this command to restore to default setting.

spanning-tree priority *PRIORITY*

no spanning-tree priority

Syntax Description	
PRIORITY	The bridge priority and bridge MAC Address together form the Spanning-Tree Bridge-ID, which is an important factor in the Spanning-Tree Topology. The range is 0 to 61440.

Default *PRIORITY*: 32768

Command Mode Global configuration

Usage Guideline Bridge Priority is one of the two parameters used to select the Root Bridge. The other parameter is the system's MAC address.

The bridge priority value must be divisible by 4096, and a lower priority value (number) represents a higher priority.

This configuration will take effect only when using STP version and RSTP mode. In MSTP mode, use the command “spanning-tree mst priority” on page 852 to configure the priority for an MSTP instance.

Example This example shows how to configure the STP bridge priority to 4096.

```
Switch(config)# spanning-tree priority 4096
```

Verify the settings by entering the **show spanning-tree** command

spanning-tree tcnfilter

To enable Topology Change Notification (TCN) filtering at the specific interface, use **spanning-tree tcnfilte**r command at the interface mode. Use the no form of this command to disable TCN filtering.

spanning-tree tcnfilter

no spanning-tree tcnfilter

Syntax None

Default Disabled

Command Mode Interface configuration

Usage Guideline Both physical ports and port-channel interfaces are valid for this command.

TCN filtering can be set to enabled or disabled. If set to enabled, it stops the port from propagating received topology change notifications and topology changes to other ports.This configuration takes effect on any spanning-tree mode types.

Example This example shows how to configure TCN filtering on eth3.7.

```
Switch(config)#interface eth3.7
Switch(config-if)#spanning-tree tcnfilter
```

Verify the settings by entering the **show spanning-tree interface** command.

spanning-tree transmit hold-count

This setting is used to limit the maximum BPDU transmission rate for every port.

spanning-tree transmit-hold-count *VALUE*

Syntax Description	
VALUE	Specifies the value to restrict the numbers of BPDU transmitted on a port within the Hello Time period. The range is 1 to 10.

Default *VALUE*: 6

Command Mode Global configuration

Usage Guideline The transmission of BPDU on a port is controlled by a counter. The counter is incremented on every BPDU transmission, and decremented once each second. The transmissions are paused for one second, if the counter reaches the transmit hold count.This parameter will be is used in common by STP, RSTP, and MSTP.

Changing this parameter to a higher value may have a significant impact on CPU utilization, especially in MSTP mode. Lowering this parameter could slow convergence in some scenarios. We recommend that to not change the value from the default setting.

Example This example shows how to configure the transmit-hold-count value.

```
Switch(config)# spanning-tree transmit-hold-count 5
```

Verify the settings by entering the **show spanning-tree** command.

speed

Use this command to configure the physical port interface speed/duplex setting.

speed {10|100|1000[master|slave]|auto}

Syntax Description	
10	Specifies to set the port speed to transmit at 10 Mbps.
100	Specifies to set the port speed to transmit at 100 Mbps.
1000	Specifies to set the port speed to transmit at 1000 Mbps. • **copper port**: If the speed is set to 1000 Mbps, then the port must be manually set as either a master or a slave port. • **fiber port** (1000SX/LX): no-negotiation should be configured (i.e. auto-negotiation disable).
master	(**1000** only) Manually sets a copper port to be the master port.
slave	(**1000** only) Manually sets a copper port to be the slave port.
auto	Specifies to determine the speed through auto-negotiation with its linked partner. • **copper port**: Specify to determine the speed via auto-negotiation with its linked partner. • **fiber port**(1000SX/LX): auto-negotiation enable,auto-negotiation will be started to negotiate the clock and flow control.

Default

It will be auto for 100TX and 1000TX.

It will be fixed to 100 for 100FX.

It will be fixed to 1000 for 1000SX/LX.

Command Mode

Interface configuration

Usage Guideline

Only physical port interfaces are valid for this configuration.

If the specified speed is not supported by the hardware, error messages will be returned.

1000SX/LX is always fixed to 1000 and full duplex.

100FX is always fixed 100 and full duplex.

For all SFP/XFP modules, duplex command will not take effect.

Auto-negotiation will be enabled whether the speed is set to auto or duplex is set to auto. If the speed is set to auto, and duplex is set to fixed mode, then only the speed will be negotiated. The advertised capability will be the configured duplex mode combined with all possible speeds. If speed is to set to a fixed speed and duplex is set to auto, then only duplex mode is negotiated. The advertised

capability will consist of both the full and half duplex mode combined with the configured speeds.

Before adding ports to a Port-Channel, verify that all settings are the same on these ports. Otherwise the ports in a Port-Channel with different settings will operate in an indeterminate manner.

In IEEE 802.3 (Clause 40) 1000BASE-T standard, Auto-Negotiation is defined as necessary. Although we still provide a command to disable auto-negotiation for 1000BASE-T, setting it to enabled is recommended to prevent an unexpected link status.

Example

This example shows how to configure interface eth3.24 to force the settings to a speed of 100Mbits and auto-negotiate to the duplex mode:

```
Switch(config)# interface eth3.24
Switch(config-if)# speed 100
Switch(config-if)# duplex auto
```

Verify the settings by entering the **show interface** command.

storm-control (Interface)

Use this command to configure the device to prevent storm attacks on a LAN. There are three traffic types, broadcast, multicast, and unicast (DLF). Use the no form of the command to disable the storm-control function.

storm-control {broadcast | multicast | unicast}

no storm-control {broadcast | multicast | unicast}

Syntax Description	
broadcast	Set Broadcast rate limiting
multicast	Set Multicast rate limiting
unicast	Set Unicast(DLF) rate limiting

Default Disabled (all storm types)

Command Mode Interface configuration

Usage Guideline Only physical port interfaces are valid for this command.

Enter the "storm-control" command to enable Storm Control for a specific traffic type on the interface.

All packets are passed in default without storm control enabled. After enabling traffic storm control, if the storm-control action is to drop, then packets exceeding the level will be dropped. If the storm-control action is set to shutdown, then the interface will be shutdown whenever the packets exceed the threshold.

Examples This example shows how to enable Broadcast storm control on interface eth3.1.

```
Switch# configure terminal
Switch(config)# interface eth3.1
Switch(config-if)# storm-control broadcast
Switch(config-if)# show storm-control interface broadcast
Interface Storm Action Type Threshold
------------------------------------------------------------
eth3.1 Broadcast Drop pps 131072
```

This example shows how to disable Broadcast storm control. on interface eth3.1.

```
Switch# configure terminal
Switch(config)# interface eth3.1
Switch(config-if)# no storm-control broadcast
```

Verify the settings by entering the **show storm-control** interface command.

storm-control action (Interface)

This command configures the action type for the Storm Control function. It is only used for two traffic types, broadcast and multicast. Use the no form of the command to return to the default settings.

storm-control {broadcast | multicast} action {drop | shutdown}

no storm-control {broadcast | multicast} action

Syntax Description	
Broadcast	Set Broadcast rate limiting
Multicast	Set Multicast rate limiting
action drop	To drop traffic on the port when a storm occurs.
action shutdown	To shutdown the port when a storm occurs.

Default **action drop**

Command Mode Interface configuration

Usage Guideline Only physical port interfaces are valid for this command.

All packets are passed by default. After enabling traffic storm control, if storm-control action is drop, packets exceeding the level will be dropped. However if the storm-control action is set to shutdown, then the interface will be shutdown upon packets exceeding the level setting.

The Shutdown action is only available for broadcast and multicast storm control.

For unicast storm control, the software level is unable to identify unknown unicast (DLF) storm events due to the hardware chip being unable support this function. Therefore, if unknown unicast packets exceed the set level, they will always be dropped.

Examples This example shows how to configure Broadcast storm control action by setting a shutdown action on interface eth3.1. In this situation, the threshold level is not specified and the default threshold is 131072 PPS.

```
Switch# configure terminal
Switch(config)# interface eth3.1
Switch(config-if)# storm-control broadcast action shutdown

Switch(config-if)# show storm-control interface broadcast
Interface     Storm         Action          Type              Threshold
-------------------------------------------------------------
eth3.1       Broadcast     shutdown         pps               131072
```

This example shows how to configure Broadcast storm control action and level. It assigns the shutdown action and rising threshold to 900 pps for interface eth3.1.

```
Switch# configure terminal
Switch(config)# interface eth3.1
Switch(config-if)# storm-control broadcast action shutdown
Switch(config-if)# storm-control broadcast level pps 900

Switch(config-if)# show storm-control interface broadcast
Interface     Storm         Action          Type              Threshold
------------------------------------------------------------
eth3.1       Broadcast     shutdown         pps               900
```

This example shows how to return to the default setting for Broadcast storm control action on interface eth3.1.

```
Switch# configure terminal
Switch(config)# interface eth3.1
Switch(config-if)# no storm-control broadcast action
```

Verify the settings by entering the **show storm-control** interface command.

storm-control level (Interface)

This command configures the rising threshold for Storm Control function. Use no command to return the default settings.

storm-control {broadcast | multicast | unicast} level {*LEVEL* **| pps** *PPS***}**

no storm-control {broadcast | multicast | unicast} level

Syntax Description	
Broadcast	Set Broadcast rate limiting
Multicast	Set Multicast rate limiting
Unicast	Set Unicast(DLF) rate limiting
level *LEVEL*	Specifies the rising threshold as a percentage (0 to 100) of total bandwidth of the port.
level pps *PPS*	Specifies the rising threshold as a rate in packets per second at which traffic is received on the port. The range of PPS is from 1 to 148810 (for 100 Mbps). For 1000 Mbps, the range is 1 to 1488100 and so on.

Default **level pps** *PPS*: 131072 packets per second

Command Mode Interface configuration

Usage Guideline Only a physical port interface is valid for this command.

The precise suppression level, as a percentage (0 to 100) of total bandwidth of specific port interface, is not able to be calculated exactly. That is, the current calculation formula assumes that the packet size of all incoming packets is 1512 bytes.

Examples This example shows how to configure Broadcast storm control LEVEL by pps mode. It assigns the pps threshold level of interface eth3.1 for incoming broadcast packets to 500 and drops the packets that exceed the threshold.

```
Switch# configure terminal
Switch(config)# interface eth3.1
Switch(config-if)# storm-control broadcast level pps 500

Switch# show storm-control interface broadcast

Interface     Storm         Action          Type              Threshold
-------------------------------------------------------------
eth3.1       Broadcast     Drop              pps             500
```

This example shows how to configure the Broadcast storm control LEVEL by percentage mode. It assigns the percentage threshold level of interface eth3.1 for incoming broadcast packets to 90 and drops the packets that exceed the threshold.

```
Switch# configure terminal
Switch(config)# interface eth3.1
Switch(config-if)# storm-control broadcast level 90

Switch(config-if)# show storm-control interface broadcast
Interface     Storm         Action          Type              Threshold
------------------------------------------------------------
eth3.1       Broadcast     Drop             percentage       90
```

This example shows how to return to the default setting for Broadcast storm control level on interface eth3.1.

```
Switch# configure terminal
Switch(config)# interface eth3.1
Switch(config-if)# no storm-control broadcast level

Switch(config-if)# show storm-control interface broadcast
Interface     Storm         Action          Type              Threshold
------------------------------------------------------------
eth3.1       Broadcast     Drop              pps             131072
```

Verify the settings by entering the **show storm-control interface** command

storm-control timer (Global)

Use this command to configure the timer options. The timers are used to implement a storm control shutdown action. Use the no form of the command to return the default settings.

storm-control { time-interval *SECONDS* **| countdown** *SECONDS* **| auto-recover-time** *SECONDS* **}**

no storm-control { time-interval | countdown | auto-recover-time}

Syntax Description	
time-interval *SECONDS*	Software will monitor the counter of received broadcast or multicast packets periodically based on this user defined interval. The range of the checking interval (*SECONDS*) is from 5 to 30 seconds.
countdown *SECONDS*	If a port is in shutdown mode and this timer runs out, the port will be placed in shutdown forever mode. If the value is '0' the function of shutdown forever is disabled. The valid range for this setting is 0, 180 - 1800 seconds.
auto-recover-time *SECONDS*	Specifies the time that a port is in shutdown forever mode, from which it can be automatically recovered. When the value is set to '0' a port cannot recover from forever shutdown. The valid range for this setting is 0, 300 - 1800 seconds.

Default

time-interval *SECONDS*: 5 seconds

countdown time *SECONDSr*: 0 seconds

auto-recover-time *SECONDS*: 0 seconds

Command Mode

Global configuration

Usage Guideline

If the action option is set to shutdown, the port will enter shutdown mode (i.e. the port is blocked) when the threshold is exceeded. If the traffic rate has been higher than the threshold for a configurable period (countdown timer), the port will enter into shutdown forever mode (i.e. the port is disabled and the status is link-down).

When a port is in "shutdown mode", before the port enters into shutdown forever mode it can recover and the port will exit the shutdown mode. if the receiving rate is higher than the falling threshold (80% of the threshold), and lower than the threshold, the port will exit the shutdown mode after a period of time and the timer will then be half of the **countdown** timer.

Furthermore, if the receiving rate is lower than the falling threshold the port will be recovered immediately.

If the **auto_recover_time** value is non-zero, the port will be automatically recovered to the normal situation after the recovery time. Otherwise, the port will

not be automatically recovered but it can be manually recovered by using the "no shutdown" command.

Examples

This example shows how to configure the **time-interval**. The count of received broadcast or multicast packets is monitored every 15 seconds.

```
Switch# configure terminal
Switch(config)# storm-control time-interval 15
Switch(config)#
```

This example shows how to configure the **countdown** timer. When the threshold is exceeded, the port will enter into the shutdown mode. If the traffic rate has been higher than the threshold during the count of 180 seconds, then the port will be changed to shutdown forever mode.

```
Switch# configure terminal
Switch(config)# storm-control time-interval 15
Switch(config)# storm-control countdown 180
Switch(config)#
```

This example shows how to configure the **auto-recovery-timer**. When a port is in shutdown forever mode, it will be automatically recovered to normal operation after 300 seconds.

```
Switch# configure terminal
Switch(config)# storm-control time-interval 15
Switch(config)# storm-control countdown 180
Switch(config)# storm-control auto-recover-time 300
Switch(config)#
```

Verify the settings by entering the **show storm-control** command

subnet-base (VLAN)

Use the subnet command to specify a subnet-based VLAN ID assignment for untagged incoming packets. Use the no form of this command to remove a subnet-based VLAN ID entry setting.

subnet-base { *NETWORK-PREFIX NETWORK-MASK* | *NETWORK-PREFIX / PREFIX-LENGTH* **}**

no subnet-base { *NETWORK-PREFIX NETWORK-MASK* | *NETWORK-PREFIX / PREFIX-LENGTH* **}**

Syntax Description	
NETWORK-PREFIX NETWORK-MASK	The network prefix and the network mask specify the destination network in the form of A.B.C.D xxx.xxx.xxx.xxx.
NETWORK-PREFIX/ PREFIX-LENGTH	The network prefix and the prefix length specify the destination network in the form of A.B.C.D/x.

Default Not configured

Command Mode VLAN configuration

Usage Guideline A subnet VLAN entry is an IP subnet-based VLAN classification rule. If an untagged or priority-tagged IP packet is received on a port, its source IP address will be used to match the subnet VLAN entries. If the source IP matches the subnet of an entry, the packet will be classified to the VLAN of this entry. The number of subnet-based VLAN entries is project dependent.

Example This example shows how to create a subnet-based VLAN entry.

```
Switch(config)#vlan 100
Switch(config-vlan)#subnet-base 20.0.1.0/8
Switch(config-vlan)#subnet-base 192.0.1.0/8
Switch(config-vlan)#end
```

Verify the settings by entering the **show vlan** command.

subnet-mask

Use this command to configure the subnet mask for a DHCP address pool of the DHCP Server. Use the no form of this command to restore the configuration of a subnet mask to the default mask 255.255.255.0.

subnet-mask *MASK*

no subnet-mask

Syntax Description	
MASK	The bit combination of the addresses, in the DHCP address pool, determines which part of the address refers to the network or subnet and which part refers to the host. It is in the format of xxx.xxx.xxx.xxx in which xxx is the number range from 0 to 255 where all of its binary bits must be continuous.

Default *MASK*: 255.255.255.0

Command Mode DHCP pool configuration

Usage Guideline This command configures the subnet mask that the DHCP server is uses to assign to DHCP clients. It is valid for the associated DHCP address pools only.

Examples The following is an example of configuring 255.0.0.0 as the DHCP pool's subnet mask .

```
switch#configure terminal
switch(config)#ip dhcp pool pool1
switch(config-dhcp)#subnet-mask 255.0.0.0
switch(config-dhcp)#
```

switchport port-security

Use this command to configure port security setting of a specified port interface to restrict the allowable number of users that can gain access to the port.

Use the no form of the command to disable the port security, or delete user-defined secure MAC address.

switchport port-security [maximum *VALUE* **| violation {protect | shutdown} | mode {permanent | delete-on-timeout}]**

no switchport port-security

Syntax Description	
maximum *VALUE*	(Optional) Specifies the maximum allowable number of secure MAC addresses (users) The range for the VALUE is project dependent.
violation {protect | shutdown}	(Optional) Specifies the action to be taken when a security violation is detected: **protect**: Drops all the packets from the insecure hosts at the port-security process level but does not increment the security-violation count. **shutdown**: Shutdown the port if there is a security violation.
mode { permanent | delete-on-timeout }	Specifies the port security mode: The different option keywords are described below: **permanent**: This mode defines that all learnt MAC addresses will not be purged unless a user deletes those entries manually. **delete-on-timeout**: Setting this mode defines that all learnt MAC addresses will be purged when an entry is aged-out or a user deletes these entries manually.

Default

Disabled

maximum *VALUE*: 1

mode: **delete-on-timeout**

violation: **shutdown**

Command Mode

Interface configuration at Privilege level 15

Global configuration with Privilege level 15 (only for a **no port-security** command).

Usage Guideline

The valid interface for this configuration is a physical port.

The VLAN does not need to exist for the command to succeed.

When the mode is permanent, the learned entries will be stored automatically and restored after a reboot.

If a port-security command is issued without specifying any arguments, then the port security feature will be enabled with the default settings for the maximum and mode parameters.

As the port-security state is changed from disabled to enabled or vice versa, the auto-learned MAC entries are cleared,

If no arguments are specified when issuing the no port-security command, then the port security feature will be disabled.

If the no port-security command, without any options, is applied in global configuration mode, then it will set the port-security to disabled for all ports.

When the mode setting is changed, the addresses, both originally learned and configured entries on the port, will be cleared.

When the maximum setting is changed, the learned address will remain unchanged when the maximum number increases; the learned address will be cleared when the number is decreased.

A port-security enabled port has the following restrictions.

- The port security function cannot be enabled simultaneously with dot1x which provides more advanced secure capability.
- A port which is in private-vlan mode can not enable port-security.
- If a port is specified as the destination port for the mirroring feature, then the port-security function can not be enabled.
- If a port is the member port of a channel group, then it cannot be enabled with the port-security function.

The system will periodically check whether the secured count is changed within 1 minute intervals.

When a security violation is detected, one of the following actions occurs:

- *Protect* - When the number of port-secure addresses reaches the maximum limit that is allowed on the port, the packets with unknown source addresses are dropped until they have a sufficient number of secure MAC addresses manually removed.
- *Shutdown* - The interface is error disabled when a security violation occurs

The security-violation count is accumulated and based on the different number of MAC addresses which violate the secured port.

Note- When a secure port is in the error-disabled state, it can be manually re-enabled by entering **no shutdown** commands in interface-configuration mode

The no form of the command can be used in global coniguration so that one command can use then disable port-security at all ports.

Examples

This example shows how to configure port security in **permanent** mode with maximum number 5.

```
Switch# configure terminal
Switch(config)# interface eth3.1
Switch(config-if)# switchport port-security mode permanent
Switch(config-if)# switchport port-security maximum 5
Switch(config-if-range)# end
```

This example shows how to set the action to be taken when a security violation is detected:

```
Switch# configure terminal
Switch(config)# interface eth3.1
Switch(config-if)# switchport port-security violation protect
Switch(config-if-range)# end
```

Verify the settings by entering the **show port-securit**y command

synchronization

To enable the synchronization between Border Gateway Protocol (BGP) and an external Interior Gateway Protocol (IGP) system, use the synchronization command. To advertise a network route without waiting for the IGP, use the no form of this command.

synchronization

no synchronization

Syntax None

Default Disabled

Command Mode Router configuration

Address family configuration

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 an IGP is disabled 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 the other routers in an autonomous system do not speak BGP.

Example This example shows how to enable synchronization in AS 65121.

```
Switch(config)# router bgp 65121
Switch(config-router)# synchronization
Switch(config-router)#
```

system-name

Use this command to configure the system name information. Use the **no system-name** command to set the system name to a null string.

system-name *TEXT*

no system-name

Syntax Description	
TEXT	Specifies the string that describes the system name information. The maximum length is 128 characters. The syntax is a general string that allows space.

Default Not configured

Command Mode Global configuration

Usage Guideline Configure the system name information on the switch.

Example This example shows how to set up the system name information with the string DGS-6604 Chassis Switch.

```
Switch(config)# system-name DGS-6604 Chassis Switch
```

Verify the settings by entering the **show snmp-server** command.

telnet

The telnet command is used to login in another device that supports the TELNET protocol.

telnet {*IP-ADDRESS* | *IPV6-ADDRESS}* *[TCP-PORT]*

Syntax Description	
IP-ADDRESS	IPv4 address of the host.
IPV6-ADDRESS	IPv6 address of the host.
TCP-PORT	Specifies the The TCP port number that telnet should use. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the TELNET protocol is 23.

Default *TCP-PORT*: 23

Command Mode Management interface or User EXEC

Usage Guideline This command starts the telnet client function and can be used to communicate with another device using the TELNET protocol. The telnet command is allowed under both management interface modes and User EXEC mode. For User EXEC mode, the outgoing physical interfaces does not include the management interface. To use telnet in order to login to a device which can be reached only through the management port, use the telnet command under management interface mode by entering the mgmt-if command first.

The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is Ctrl-_ (press and hold the Ctrl and Shift keys and the '_' key, the underscore). The special Telnet commands will be displayed as follows:

Supported commands are:

```
e - terminate the current Telnet session
```

If any other key is pressed, the terminal will return to the original active Telnet session.

Use the lowercase letter, 'e' to exit from the telnet software.

Several concurrent Telnet sessions can be opened on the switch system and each open Telnet session can have its own telnet client software concurrently supported.

Use "ctrl-c" to stop the connection if telnet is connecting but before the session connection is made.

Examples

The following example shows how to telnet to the IP address 20.74.19.200 with default port 23 (optional port parameter is provided). The IP address of 20.74.19.200 is the management interface which allows users to log in.

```
Switch#telnet 20.74.19.200
Connecting to 20.74.19.200 ...
Connected to 20.74.19.200.
Escape character is 'Ctrl-_'.

Telnet connecting ...
                          Chassis-based High-Speed Switch
                              Command Line Interface
                               Firmware: 1.00.029
          Copyright (c) 2010 D-Link Corporation. All rights reserved.
Switch>
```

The following example first shows a telnet session connecting to IP address 20.74.19.200 with default port 23, but the connection fails. The example then retries using TCP port 3500 instead at the same IPaddress 20.74.19.200 which is the management interface and logs in successfully.

```
Switch#telnet 20.74.19.200
Connecting to 20.74.19.200 ...
Could not open connection to the host, on port 23: Connection refused
Switch#

Switch#telnet 20.74.19.200 3500
Connecting to 20.74.19.200 ...
Connected to 20.74.19.200.
Escape character is 'Ctrl-_'.

Telnet connecting ...
                          Chassis-based High-Speed Switch
                              Command Line Interface
                               Firmware: 1.00.029
          Copyright (c) 2010 D-Link Corporation. All rights reserved.
Switch>
```

The following example shows a telnet session attempting to connect to IP address 10.74.19.2, but the IP adress is not reachable.

```
Switch#telnet 10.74.19.2
Connecting to 10.74.19.2 ...
Could not open connection to the host, on port 23: Network is unreachable
Switch#
```

The following example shows how to enter the management interface mode and telnet to the IP address 20.74.19.200 with default port 23. Then the example shows how to exit the telnet session by entering the escape sequence : Ctrl-_ and then followed by the 'e' key.

```
Switch#configure terminal
Switch(config)#mgmt-if
Switch(mgmt-if)#telnet 20.74.19.200
Connecting to 20.74.19.200 ...
Connected to 20.74.19.200.
Escape character is 'Ctrl-_'.

Telnet connecting ...
                          Chassis-based High-Speed Switch
                              Command Line Interface
                               Firmware: 1.00.029
          Copyright (c) 2010 D-Link Corporation. All rights reserved.
Switch>
Supported commands are:
 e -            terminate the current Telnet session
If other key is pressed, the terminal will return to the original active
Telnet session.

The telnet is disconnected.
Switch(mgmt-if)
```

The following example show how to telnet to the IP address 20.74.19.200 with default port 23, then enter the escape sequence : Ctrl-_ and press any other key returning to the telnet session.

```
Switch#telnet 20.74.19.200
Connecting to 20.74.19.200 ...
Connected to 20.74.19.200.
Escape character is 'Ctrl-_'.

Telnet connecting ...
                          Chassis-based High-Speed Switch
                              Command Line Interface
                               Firmware: 1.00.0029
          Copyright (c) 2010 D-Link Corporation. All rights reserved.
Switch>
Supported commands are:
 e -            terminate the current Telnet session
If other key is pressed, the terminal will return to the original active
Telnet session.

continuing...
Switch>
```

The following example show how to telnet to the IPv6 address 2001:e10:5c00:2::101:253 using default port 23, then enter the escape sequence : Ctrl-_ and press any other key returning to the telnet session.

```
Switch#telnet 2001:e10:5c00:2::101:253
Connecting to 2001:e10:5c00:2::101:253 ...
Connected to Telnet connecting ...
Escape character is 'Ctrl-_'.

Telnet connecting ...

                        Chassis-based High-Speed Switch
                             Command Line Interface
                              Firmware: 1.00.029
          Copyright (c) 2010 D-Link Corporation. All rights reserved.
Switch>
Supported commands are:
 e -            terminate the current Telnet session
If other key is pressed, the terminal will return to the original active
Telnet session.

continuing...
Switch>
```

The following example show how to telnet to the IPv6 address 2001:e10:5c00:2::101:253 with specific port 3500.

```
Switch#telnet 2001:e10:5c00:2::101:253 3500
Connecting to 2001:e10:5c00:2::101:253 ...
Connected to Telnet connecting ...
Escape character is 'Ctrl-_'.

Telnet connecting ...
                         Chassis-based High-Speed Switch
                             Command Line Interface
                              Firmware: 1.00.029
          Copyright (c) 2010 D-Link Corporation. All rights reserved.
Switch>
```

terminal length

This command configures the number of lines to be displayed in the monitor output. The terminal length command will only affect the current session. If option **default** is specified, the display length will be applied to all sessions.

terminal length *LINES* **[default]**

no terminal length

Syntax Description	
LINES	Number of lines to display on the screen; valid values are from 0 to 512.
default	(Optional) Sets the number of lines in the terminal display for the current administration session and all other sessions subsequently opened (Privileged EXEC only).

Default *LINES*: 24

Command Mode User EXEC

Usage Guideline When the terminal length is specified to 0, the display will not stop until it reaches the end of the display.

If terminal length is specified to a value other than 0, for example 50, then the display will stop for every 50 lines. Terminal length is to set the number of lines displayed on the current terminal screen. This command also takes effect tfor both Telnet and SSH sessions automatically. .

Output from a single command that overflows a single display screen is followed by the --More-- prompt. At the --More-- prompt, press Ctrl-C, q, or Q to interrupt the output and return to the prompt, press the Spacebar to display an additional screen of output, or press Return to display one more line of output.

Setting the **terminal length** to 0 turns off the scrolling stop feature and causes the entire output to display at once (continuously).

Unless the **default** keyword is specified, changing the terminal length value applies only to the current session. When changing the value in a session, the value applies only to that session. When using the no form of this command, the number of lines in the terminal display is reset to the default of 24.

The **default** keyword is available in Privileged EXEC mode only.

Example This example shows how to change the lines to be displayed in a screen to 60.

```
Switch# terminal length 60
```

terminal timeout

Use this command to setup a timeout value, which upon its expiry, will auto-logout the terminal session .

terminal timeout {never| 2_minutes| 5_minutes| 10_minutes| 15_minutes}

Syntax Description	
never	Specifies that the terminal session will never timeout.(the default setting).
2_minutes	Specifies that when the session is idle over 2 minutes, the terminal will auto logout.
5_minutes	Specifies that when the session is idle over 5 minutes, the terminal will auto logout.
10_minutes	Specifies that when the session is idle over 10 minutes, the terminal will auto logout.
15_minutes	Specifies that when the session is idle over 15 minutes, the terminal will auto logout.

Default **never**

Command Mode Privilege EXEC

Usage Guideline This timer specifies the length of the session idle time allowed. After this idle timer expires then the terminal session will be auto-logged out. The timer operates regardless of whether the session is established by direct serial connection, telnet connection, or SSH connection.

Examples This example shows how to setup the terminal session to never timeout.

```
Switch# terminal timeout never
```

Verify the settings by entering the **show running-config** command.

terminal width

This command sets the number of character columns on the terminal screen for the current lines displayed in a session. The **terminal width** command will only affect the current session. If option **default** is specified, the display length will be applied to all subsequent sessions and will be stored in the system configuration (start-up config) to retain the setting for the next system restart.

terminal width *CHARACTERS* **[default]**

no terminal width

Syntax Description	
CHARACTERS	Specfies the number of characters to display on the screen; valid values are from 80 to 255.
Default	**default** (Optional) Sets the number of columns in the terminal display screen for the current administration session and all other subsequent sessions. This setting can be saved into the system configuration file (start-up config) and retained for the next system restart (Privileged EXEC only).

Default *CHARACTERS*: 80 characters

Command Mode User EXEC

Usage Guideline By default, the switch system terminal provides a screen display width of 80 characters. Reset this value for the current session if it does not meet the needs of required for the terminal display.

Unless the default keyword is used, a change to the terminal width value applies only to the current session. When the value in a session is changed, the value applies only to that session. When the no form of this command is used, then the number of lines in the terminal display screen is reset to the default of 80 characters.

For a remote CLI session access such as Telnet, the auto negotiation result of terminal width will take precedence over the global configuration if the negotiation is successful. Otherwise, the global configuration takes effect. After that, adjust the line and width for the current session (this change will not be saved in the system configuration for the next system restart). This will not affect other sessions or the global configuration.

When exiting from the current session, the values of the terminal line and width is reset back to the system configuration values (it may not be same as the default setting, 80 characters; it is dependant on the current system configuration setting).

Examples The following example shows how to adjust the current session terminal width to 120 characters. The system terminal setting is not affected by the change. That is because the adjustment is only applied to the current session.

```
Switch#terminal width 120
```

The following example shows how to adjust the terminal session width to 120 as the system configuration setting for terminal width. This setting will affect all subsequently opened terminal sessions.

```
Switch#terminal width 120 default
```

timers

Use this command to configure the RIP network timers. To restore the default timers use the default form of this command.

timers {update *SECONDS* **| invalid** *SECONDS* **| flush** *SECONDS* **}**

default timers {update | invalid | flush}

Syntax Description	
update *SECONDS*	Specifies the rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the RIP routing protocol. The default is 30 seconds. The range is 5 to 2147483647 (signed long).
invalid *SECONDS*	Specifies the Interval of time (in seconds) after which a route is declared invalid. It should be at least three times the value of the update argument. A route becomes invalid when there is an absence of updates that refresh the route. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 180 seconds. The range is 5 to 2147483647.
flush *SECONDS*	Specifies the amount of time (in seconds) that must pass before the route is removed from the routing table. The default is 120 seconds. The range is 5 to 2147483647.

Default

update *SECONDS*: 30

invalid *SECONDS*: 180

flush time *SECONDS*: 120

Command Mode

Router configuration

Usage Guideline

The basic timing parameters for RIP are adjustable. RIP executes a distributed, asynchronous routing algorithm, therefore these timers must be the same for all routers and access servers in the network.

Example

The following example shows how to configure the update timer to 60 seconds:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# timer update 60
```

Verify the settings by entering the **show ip protocols** command.

timers basic

To configure update, timeout, and garbage-collection timers for an IPv6 RIP routing process, use the **timers basic** command. To return the timers to their default values, use the no form of this command.

timers basic *update timeout garbage-collection*

no timers basic

Syntax Description	
update	Specifies the interval of time in seconds at which updates are sent. This is the fundamental timing parameter of the RIP IPv6 routing protocol. The value is from 5 to 2147483647.
timeout	Specifies the interval of time in seconds after which a route is declared invalid. The route becomes invalid when there is an absence of updates that refresh the route. However, the route is still used for forwarding packets.The value is from 5 to 2147483647.
garbage-collection	Specifies the amount of time in seconds that must pass from when a route becomes invalid until the route is removed from the routing table.The value is from 5 to 2147483647.

Default

update *SECONDS*: 30

timeout *SECONDS*: 180

garbage-collection *SECONDS*: 120

Command Mode

Router configuration

Usage Guideline

The **timers basic** command is similar to the command **"timers" on page 882**.

Use the update argument to set the time interval between RIP routing updates. If no route update is received for the time interval specified by the timeout argument, the route is considered unreachable. The use of a timeout interval is not recommended for RIP because it can introduce long delays in convergence.

Use the garbage-collection argument to specify the time interval between a route being considered invalid and the route being purged from the routing table.

The basic timing parameters for IPv6 RIP are adjustable. IPv6 RIP is executing a distributed, asynchronous routing algorithm, therefore it is important that these timers be the same for all routers and access servers in the network.

Examples

The following example (on the next page) sets updates every 5 seconds. If a route is not heard from in 15 seconds, the route is declared invalid. Assuming no updates, the route is flushed from the routing table 30 seconds after the end of the hold-down period.

```
Switch > enable
Switch # configure terminal
Switch (config) # router ipv6 rip
Switch (config-router)# timers basic 5 15 30
```

timers bgp

Use this command to adjust BGP network timers. Use the **no** form of this command to restore the timers to the default value.

timers bgp *KEEP-ALIVE* **[** *HOLD-TIME* **]**

no timers bgp

Syntax Description	
KEEP-ALIVE	Specifies the frequency, in seconds, with which the switch sends KEEPALIVE messages to its BGP peer. The range is from 0 to 65535.
HOLD-TIME	(Optional) Specifies the interval, in seconds, after not receiving a KEEPALIVE message that the switch 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.

Usage Guideline

The suggested default value for the KEEPALIVE is one third (1/3) of the HOLDTIME. The timers configured for a specific neighbor or peer group (by the command **"neighbor timers" on page 438**) overrides 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*.

Example

This example shows how to change the *KEEP-ALIVE* timer to 50 seconds and the *HOLD-TIME* timer to 150 seconds:

```
Switch(config)# router bgp 65100
Switch(config-router)# timer bgp 50 150
```

time-range

Use this command to enter the time range configuration mode to define a time range. Use the no form of the command to delete a time range.

time-range *NAME*

no time-range *NAME*

Syntax Description	
NAME	Specifies the name of the time-range profile to be configured. It can accept up to 32 characters. The syntax is a general string that does not allow space.

Default None

Command Mode Global configuration

Usage Guideline Use this command to enter the time range configuration mode before using the command **"periodic" on page 457** to specify the time period.

If **time-range** is used by access-list rules, it cannot be deleted and an error message will be shown as below:

Warning! The time-range can not be deleted because it is in use

Examples This example shows how to enter the time range configuration mode for the time-range profile, named *trange1*.

```
Switch(config)# time-range trange1
```

This example shows how to remove time-range profile, named *offtime*, which has been associated to an IP access-list, *Sales.*

```
Switch(config)# no time-range offtime
Warning! The time-range can not be deleted because it is in use.
```

Verify the settings by entering the **show time-range** command.

traceroute

To display a hop-by-hop path through an IP network from the switch to a specific destination host, use the **traceroute** command.

traceroute [*OPTIONS***] { *IP-ADDRESS* | *IPV6-ADDRESS*}**

Syntax Description	
OPTIONS	(Optional) the option can be any combination of the following parameters: **-w** *WAIT_TIME* Optionally used to specify the amount of time (in seconds) that traceroute will wait for an ICMP response message. The allowed range for *WAIT_TIME* is from 1 to 300 seconds. **-i** *INITIAL_TTL* Optional setting that causes traceroute to send ICMP datagrams with a TTL value equal to *INITIAL_TTL* instead of the default TTL of 1. This option causes traceroute to skip processing for hosts that are less than *INITIAL_TTL* hops away. **-m** *MAX_TTL* Optional setting used to specify the maximum TTL value for outgoing ICMP datagrams. The allowed range for *MAX_TTL* is from 1 to 255. **-p** *DEST_PORT* Optionally used to specify the base UDP destination port number used in traceroute datagrams. This value is incremented each time a datagram is sent. The allowed range for *DEST_PORT* is from 1 to 65535. Use this option in the unlikely event that the destination host is listening to a port in the default traceroute port range. **-q** *NQUERIES* Optionally used to specify the number of datagrams to send for each TTL value. The allowed range for *NQUERIES* is from 1 to 1000. **-s** *PACKET_SIZE* Optionally used to specify the number of bytes in addition to the default of 40 bytes, of the outgoing datagrams. The allowed range is from 0 to 1420. **-t** *TOS* Optionally used to specify the ToS to be set in the IP header of the outgoing datagrams. The allowed range for TOS is from 0 to 255.
IP-ADDRESS	IP address in dot notation (a.b.c.d) of the destination host.
IPV6-ADDRESS	IPv6 address of the destination host.

Default

-w: 5 seconds

-i: 1

-m: 30

-p: 33434

-q: 3

-t: 0

-s: 40 bytes

Command Mode

Management interface mode or User EXEC

Usage Guideline

To interrupt **traceroute** after the command has been issued, press Ctrl-C.

The traceroute command uses the TTL field in the IP header to cause routers and servers to generate specific return messages. **traceroute** starts by sending a UDP datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an ICMP *time-exceeded* message to the sender. The **traceroute** facility determines the address of the first hop by examining the source address field of the ICMP *time-exceeded* message.

To identify the next hop, **traceroute** again sends a UDP packet but this time with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the *time-exceeded* message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To determine when a datagram has reached its destination, **traceroute** sets the UDP destination port in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram with an unrecognized port number, it sends an ICMP *port unreachable* error to the source. This message indicates to the **traceroute** facility that it has reached the destination.

Use the TOS option to see if different types of service cause routes to change.

Note : The specified *OPTIONS* can be any combination of each parameters. However, the parameters must be specified in the alphabetical order and upper case options are ahead of lower case options (similar to the PING command).

Examples

This example shows how to **traceroute** the host with IP address "172.50.71.123".

```
Switch# traceroute 172.50.71.123
traceroute to 172.50.71.123 (172.50.71.123), 30 hops max, 40 byte packets
1 172.50.71.123 (172.50.71.123)  0.847 ms  0.344 ms  0.376 ms
Switch#
```

Display Field Descriptions

The following table describes the fields in the traceroute command output.

Display Field	Description
1	Indicates the sequence number of the router in the path to the host.
172.50.71.123	Host name of this router.
(172.50.71.123)	Internet address of this router.
30 hops max, 40 byte packets	Maximum TTL value and the size of the ICMP datagrams being sent.
0.847 ms 0.344 ms 0.376 ms	Total time (in milliseconds) for each ICMP datagram (three ICMP probes per TTL for this case) to reach the router or host plus the time it took for the ICMP time-exceeded message to return to the host.

This example shows how to **traceroute** the host with IPv6 address "2001:238:f8a:77:7c10:41c0:6ddd:ecab".

```
Switch# traceroute 2001:238:f8a:77:7c10:41c0:6ddd:ecab
traceroute to 2001:238:f8a:77:7c10:41c0:6ddd:ecab
(2001:238:f8a:77:7c10:41c0:6ddd: ecab), 30 hops max, 40 byte packets
1  2001:238:f8a:77:7c10:41c0:6ddd:ecab
(2001:238:f8a:77:7c10:41c0:6ddd:ecab)  0.847 ms  0.344 ms  0.376 ms

Switch#
```

traffic-segmentation forward

Use this command to segment or restrict the flooding domain of a port to a set of specified ports. Use the **no** form of this command to remove some ports from the forwarding domain.

traffic-segmentation forward interface *INTERFACE-ID* **[, | -]**

no traffic-segmentation [forward [interface *INTERFACE-ID* **[, | -]]]**

Syntax Description	
forward	Specifies the list of egress ports as the forwarding domain.
interface *INTERFACE-ID*	Specifies the ID of an interface as the allowable interfaces to go to. The allowed interfaces include physical ports and port channels.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default No segmentation configured. All ports are in the forwarding domain.

Command Mode Interface configuration

Usage Guideline Only physical ports and port channel interfaces are valid for this configuration.

Traffic segmentation allows a VLAN to be futher divided into smaller groups of ports to provide increased security support. The flooding domain for this feature is determined by both the VLAN domain and traffic segmentation domains. This means the outgoing ports of the flooding member should be concurrently part of the VLAN and traffic segmentation.

The command **traffic-segmentation forward interface** can be entered multiple times. The interfaces will be appended into the flowing domain. Similarly, this occurs when using the **no traffic-segmentation forward interface** command. The no form of the command will remove the specified interface from the traffic-segmentation forward member list.

The traffic segmentation member list can be comprised of different interface types, for example eth3.1 can be with a port-channel in the same traffic segmentation list. If the forwarding interfaces specified by the command include a port-channel, all the member ports of this port-channel will be the forwarding interface in operation. If the specified port of the **traffic-segmentation command** is a member of a port-channel, the command will return an error message because of the different interface types.

Since a port channel is an allowed interface in the member list, traffic segmentation is on the top link aggregation module. When any traffic segment member (physical interface) is configured to be a potential aggregated link port, it should be marked as an inactive interface and it will be treated as not existing in the forward interface list. Vice versa, if any port is removed from link aggregation, the removed port should be reset back to its default factory setting.

When entering **no traffic-segmentation** without any keywords, then all ports will become the forwarding port. When entering **no traffic-segmentation forward** without the interface keyword, then all ports in forwarding port list will be removed. That is, the forwarding domain of the configured interface is empty.

Examples

This example shows how to configure traffic segmentation. It restricts the flooding domain of eth3.1 to a set of ports, which are eth4.1 - 4.6.

```
Switch# configure terminal
Switch(config)# interface eth3.1
Switch(config-if)# traffic-segmentation forward interface eth4.1-4.6
Switch(config-if)# exit
```

This example shows how to remove some ports eth4.2- 4.3 from the forwarding port list.

```
Switch# configure terminal
Switch(config)# interface eth3.1
Switch(config-if)# no traffic-segmentation forward interface eth4.2-4.3
Switch(config-if)# exit
```

Verify the settings by entering the **show traffic-segmentation** command.

trunk allowed-vlan

Use the **trunk allowed-VLAN** configuration command to set the VLAN characteristic. It sets the allowable VLANs that can receive and send traffic on the interface in tagged format. Use the **no trunk allowed-VLAN** command to remove a tagged member port from a specified VLAN.

trunk allowed-vlan *VLAN-ID* **[, | -]**

no trunk allowed-vlan [*VLAN-ID* **[, | -]]**

Syntax Description	
VLAN-ID	Specifies the VLAN to add or remove tagging members to/from it.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of VLANs. No space before and after the hyphen.

Default Not configured

Command Mode interface configuration

Usage Guideline The valid interfaces for this command can be either physical ports or port-channels.

By setting the **trunk allowed-vlan** command multiple times, a port can become a tagged member port of multiple VLANs.

If the VLAN does not exist, an error message will return to indicate it.

When this command is applied, the port will change to trunk mode. If the mode is changed, the setting for the previous mode will disappear.

When using the **no trunk allowed-vlan** command without specifying a VLAN-ID, then the port will have its tagging memberships removed from all VLANs.

Example This example shows how to set an interface eth3.1 to a tagged member of VLAN 1000.

```
Switch(config)# interface eth3.1
Switch(config-if)# trunk allowed-vlan 1000
```

Verify the settings with the **show vlan interface** command.

tunnel destination

Use the **tunnel destination** configuration command to add the destination IPv4 address for the tunnel interface. Use the **no tunnel destination** configuration command to remove it.

tunnel destination { *IPv4-ADDRESS* **}**

no tunnel destination

Syntax Description	
IPv4-ADDRESS	Specifies the IPv4 address as the the destination address for the tunnel.

Default None

Command Mode Interface configuration

Usage Guideline Use these commands to configure the destination IPv4 address for a tunnel interface.

Tunnel interfaces are valid for this command. Only manually configured tunnels need to set the tunnel destination.

Examples This example shows how to add the destination IPv4 address for the tunnel interface 2

```
Switch(config)# interface tunne 2
Switch(config-if)#tunnel destination 10.0.0.1
Switch(config-if)#
```

This example shows how to remove the destination IPv4 address for the tunnel interface 2

```
Switch(config)# interface tunne 2
Switch(config-if)#no tunnel destination
Switch(config-if)#
```

Verify the settings by entering the **show interface** command.

tunnel mode

Use the **tunnel mode ipv6ip** configuration command to manually specify an IPv6 configured tunnel. The optional parameter **6to4** or **isatap** means that tunnel type is 6to4 or ISATAP. Use the no form of the command to remove the IPv6 specification.

tunnel mode ipv6ip [6to4 | isatap]

no tunnel mode

Syntax Description	
6to4	Specifies the IPv6 tunnel is a 6to4 tunnel type.
isatap	Specifies the IPv6 tunnel type is a ISATAP tunnel type.

Default None

Command Mode Interface configuration

Usage Guideline Tunnel interfaces are valid for this command.

In automatic 6to4 and ISATAP tunnels, routers are not configured in pairs. If a tunnel interface has the tunnel destination address configured, then it will not be able to configure the tunnel type to 6to4 or ISATAP tunnel mode.

In the 6to4 tunnel, the IPv4 address embedded in the IPv6 address is used to locate the far end of the automatic tunnel. The IPv4 address of the border router is extracted from the IPv6 address that, as an example, starts with the prefix 2002::/16, where the format is 2002::IPv4-address:/48.

The ISATAP tunnel uses a unicast address that includes a 64-bit IPv6 prefix and a 64-bit interface identifier. The IPv4 address is encoded in the last 32 bits of the interface identifier. When the IPv4 address is known to be globally unique, the first 32 bits of the interface identifier is 0000:5EFE; otherwise it is 0200:5EFE. The interface identifier is created in modified EUI-64 format.

Examples This example shows how to specify an IPv6 manually configured tunnel.

```
Switch(config)# interface tunnel 2
Switch(config-if)#tunnel mode ipv6ip
Switch(config-if)#
```

tunnel source

Use the **tunnel source** configuration command to add the source IPv4 address for the tunnel interface. Use the **no tunnel source** configuration command to remove it.

tunnel source { *IPv4-ADDRESS* **}**

no tunnel source

Syntax Description	
IPv4-ADDRESS	IPv4 address.

Default None

Command Mode Interface configuration

Usage Guideline Use this command to configure the source IPv4 address for a tunnel interface.

Tunnel interfaces are valid for this command.

Examples This example shows how to add the source IPv4 address for the tunnel interface 2

```
Switch(config)# interface tunne 2
Switch(config-if)#tunnel source 10.0.0.1
Switch(config-if)#
```

This example shows how to remove the source IPv4 address for the tunnel interface 2

```
Switch(config)# interface tunne 2
Switch(config-if)#no tunnel source
Switch(config-if)#
```

Verify the settings by entering the **show interface** command.

username

Use the **username** command to create a user account, and use the no form of the command to delete the user account. For the no command, when a username is specified, a specific account is deleted.

username *NAME* **[privilege** *LEVEL***] password {plain-text| encrypted }** *PASSWORD*

no username *NAME*

Syntax Description	
NAME	Specifies the Username. Only one word can be used for the name arguement. The length is 1 to 32 characters.
privilege *LEVEL*	(Optional) Sets the privilege level for the user. The privilege level is between 0 and 15. The default value is 15 if it is not specified
plain-text *PASSWORD*	Specifies the password the user must enter to gain access to the switch. The password must be from 6 to 32 characters (the length of password in plain-text form is project dependant), can contain embedded spaces and is case-sensitive. The syntax is a general string that allows spaces.
encrypted *PASSWORD*	Specifies the password in the encrypted form based on SHA-I. For the encrypted form password, the length is fixed to 35 bytes long. The password is case-sensitive. When using the **show username** or the **show enable password** command, an encrypted password can be copied and pasted to this command option.

Default

Not configured

privilege *LEVEL*: 15

Command Mode

Global configuration at privilege level 15

Usage Guideline

This command creates user accounts with different access levels.

The command only accepts *LEVEL* 1, 2, 12, & 15. If the user specifies any other level, an error message will be displayed.

When the user logs in with level 1 and 2, the user will in the User EXEC mode. The user needs to further use the enable command to enter the Privileged EXEC mode. However, in level 1 User EXEC mode it is not allowed to directly enter the Privileged EXEC mode.

When the user logs in with a level higher than or equal to 12, the user will directly enter the Privileged EXEC mode. The Privileged EXEC mode can be either level 12 or 15.

The user can specify the password in **encrypted** form or in **plain-text** form. If it is in **plain-text** form, but password encryption is enabled, then the password will be converted to encrypted form.

The factory default setting sets the user account to an empty string. When the user account is empty, the any access will be logged in directly in the User Exec mode at the power user level. The user can further enter the Privileged Exec mode using the enable password. If the enable password is not set then the user only needs to use the command **"enable" on page 177**.

Examples

This example shows how to create a username and password pair. It assigns a username of admin with the password *mypassword*.

```
Switch(config)# username admin password plain-text mypassword
```

This example shows how to remove a user account with the username *admin*.

```
Switch(config)# no username admin
```

Verify the settings by entering the **show username** command.

version

Use this command to specify the RIP version to send and receive.

version { 1 | 2 }

Syntax Description	
1	Only RIP Version 1 packets are received and transmitted.
2	Only RIP Version 2 packets are received and transmitted.

Default Version **2**

Command Mode Router configuration

Usage Guideline This command defines the default RIP version. This version will be overridden if the version is explicitly specified for the interface (for example, interface command **"ip rip receive version" on page 306**).

Example The following example shows how to configure the RIP version to version 2.:

```
Switch# configure terminal
Switch(config)#router rip
Switch(config-router)#version 2
Switch(config-router)#exit
Switch(config)#
```

Verify the settings by entering the **show ip protocols rip** command.

vlan

Use the **vlan** configuration command to add VLANs and to enter the *config-vlan* mode. Use the **no vlan** configuration command to remove VLANs. The default VLAN with the VLAN ID 1, cannot be removed.

vlan *VLAN-ID* **[, | -]**

no vlan *VLAN-ID* **[, | -]**

Syntax Description	
VLAN-ID	Specifies the ID of the VLAN to be added, removed or configured. The valid VLAN ID range is 1 to 4094.The default VLAN with VLAN id 1 cannot be removed.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of VLANs. No space before and after the hyphen.

Default System has a default VLAN entry with VLAN ID 1.

Command Mode Global configuration

Usage Guideline Use the **vlan** global configuration command to add VLANs. The valid VLAN ID range is 1 to 4094. Entering the **vlan** command with a VLAN ID enters the config-VLAN mode. When entering the VLAN ID of an existing VLAN, a new VLAN is not created, but the VLAN parameters can be modified for that VLAN. When entering the VLAN ID of a new VLAN, the VLAN will be automatically created. A VLAN in a management domain remains unused until it is assigned one or more switch ports to the VLAN. Create a new VLAN first and then specify the module and ports later.

The **no vlan** global configuration command must be used to remove VLANs. When removing a non-existing VLAN, an error message will be sent. Default VLAN with VLAN ID 1 cannot be removed. Removing a VLAN will automatically remove all port memberships that belong to the VLAN. However if a VLAN is being associated to a port's access VLAN throught the access VLAN command, it can not be deleted.

Examples This example shows how to add a new VLAN. It assigns the new VLAN with VLAN id 1000 to 1005.

```
Switch(config)# vlan 1000-1005
Switch(config-vlan)#
```

This example shows how to remove an existent VLAN with VLAN id 1000 to 1005.

```
Switch(config)# no vlan 1000-1005
Switch(config)#
```

Verify the settings by entering the **show vlan** command.

vlan encapsulation

Use this command to encapsulate the original packet with an outer VLAN tag through from UNI to NNI. Use the no form of this command to delete the related VLAN encapsulation pairs.

vlan encapsulation *S-VID C-VID* **[, | -]**

no vlan encapsulation *C-VID* **[, | -]**

Syntax Description	
C-VID **[,	-]**	The VLAN ID list specified here refers to the inner-VID list (i.e. customer VLAN ID, C-VID list).
S-VID	The VLAN ID specified here refers to the outer-VIDs (i.e. service provider VLAN ID, S-VID).

Default No VLAN encapsulation pair is created.

Once a VLAN encapsulation pair is created, the CoS setting is set to customer CoS trusted in default.

Command Mode Interface configuration (only available for User-to-Network interface).

Usage Guideline *C-VID* **[, | -]** is a customer VLAN list. After receiving packets of these VLANs, the switch will encapsulate the packets with the specified outer VLAN tag (*S-VID*) and T-PID (set at NNI port). The priority tag of the outer tag is decided by following the following conditions:

1.If the there is a CoS remarking pair for the customer VLAN, the priority tag value of the outer VLAN value is set to the same value as the cos remarking.

2.Otherwise, the priority tag value of the outer tag is replicated from the user/ inner priority tag.

Examples In the example shown here, eth4.1 is configured as COS value of 3 and CoS value of 1 for *C-VID* 22 and customer CoS trusted for *C-VID* 23-26. In addition, *S-VID* 100 is used to encapsulate the receiving packet which has *C-VID* equal to 22-26.

```
Switch(config)#interface eth4.1
Switch(config-if)#vlan encapsulation 100 22-26
Switch(config-if)#cos remarking 3
Switch(config-if)#cos remarking 1 22
```

Verify the settings by entering **show vlan-tunnel** command.

vlan name

Use the **vlan name** *VLAN-NAME* configuration command to specify the VLAN name. Use the **no vlan name** command to reset the VLAN name to the default VLAN name.

vlan name *VLAN-NAME*

no vlan name

Syntax Description	
VLAN-NAME	Specifies the VLAN name, an ASCII string from 1 to 32 characters that must be unique within the administrative domain. The character syntax allowed is a general string that does not allow spaces.

Default *VLAN-NAME*: VLANxxxx

where xxxx represents four numeric digits (include leading zeros) equal to the VLAN id number.

Command Mode VLAN configuration

Usage Guideline Use **the vlan name** *VLAN-NAME* config-VLAN command to specify VLAN name. The VLAN name length must be 1 to 32, and it must be unique within the administrative domain. The error message will be returned if an invalid name or a duplicated name is specified. Use **no vlan name** config-VLAN command to reset the VLAN name to the default VLAN name.

Example This example shows how to set a VLAN name of VLAN 1000.

```
Switch(config)# vlan 1000
Switch(config-vlan)# vlan name admin-vlan
```

Verify the settings by entering the **show vlan** command.

vlan remarking

Use this command to define the VLAN remarking pair. Use the no form of this command to delete the related VLAN remarking pair.

vlan remarking *S-VID C-VID*

no vlan remarking *C-VID***[, | -]**

Syntax Description	
*C-VID***[,	-]**	The VLAN IDs specified here refers to the inner-VID list (i.e. customer VLAN ID, *C-VID*).
S-VID	The VLAN ID specified here refers to the outer-VIDs (i.e. service provider VLAN ID, *S-VID*).

Default

No VLAN remarking pair is created.

Once a VLAN remarking pair is created, the CoS setting is set to customer CoS trusted by default.

Command Mode

Interface configuration (only available for a UNI port)

Usage Guideline

C-VID **[, | -] i**s a customer VLAN list. After receiving packets of these VLANs, the switch will replace the VLAN tag of the packets with the specified *S-VID* VLAN tag. The priority tag of the outgoing tag is decided by following the following conditions:

1.If the *C-VID* is set as remarking priority by the **cos remarking** command, the priority tag value of the outgoing tag is decided by the configuration associated with the ingress port and inner VID.

2.Otherwise, the priority tag value of the outer VLAN value is retained as the original CoS priority tag value.

Example

This example shows how to create VLAN translation entries. The created VLAN translation relationships are: C-VLAN 200 will be translated to SP-VLAN 1002, priority is 7. And the S-TAG is added.

Please follow the example below for a step by step explanation

1. Go to interface Ethernet 4.1

```
Switch(config)#>interface eth4.1
```

2. Make a VLAN encapsulation table - *S-VID* is 1001 and *CVID* is 101-104. So far the user's COS is trusted.

```
Switch(config-if)#>vlan encapsulation 1001 101-104
```

3. Make a VLAN remarking from *C-VID* 200 to *S-VID* is 1002. So far the user's COS is trusted.

```
Switch(config-if)#>vlan remarking 1002 200
```

4. Remark COS as 7.

```
Switch(config-if)#>cos remarking 7
```

5. Remark COS as 3 for *C-VID* 101-102, remarking COS as 7 for and 103-104 and 200.

```
Switch(config-if)#>cos remarking 3 101-102
```

6. Trust user's COS for VID 200 and 103-104(that is because when *C-VID* is not specified with COS rearming policy explicitly, its COS is changed according to cos remarking NEW-COS or no cos remarking commands), but remark COS as 3 for *C-VID* 101-102.

```
Switch(config-if)#>no cos remarking
Switch(config-if)#>
```

7. Verify the settings by entering **show vlan-tunnel interface** command.

vlan-tunnel

Use this command to enable the VLAN tunnel mode. Use the no form of the command to disable the VLAN tunnel mode.

vlan-tunnel

no vlan-tunnel

Syntax None

Default Disabled

Command Mode Global configuration

Usage Guideline This command enables VLAN tunneling mode. To turn VLAN tunneling mode from disabled to enabled state. The default setting of VLAN tunneling mode is applied with the following setting:

1. All interfaces are set as Network-to-Network Interfaces (NNI) port.
2. All existing static VLANs will run as SP-VLANs. All dynamically learned L2 addresses will be cleared.
3. All dynamically registered VLAN entries will be cleared.
4. IIn order to run GVRP on the switch, enable GVRP manually. In VLAN tunnel mode, the SP-VLAN GVRP Address (01-80-C2-00-00-0D) will be used by the GVRP protocol.

Example This example shows how to enable the VLAN tunnel mode.

```
Switch# configure terminal
Switch(config)# vlan-tunnel
Switch(config)#
```

Verify the settings by entering **show vlan-tunnel** command.

vlan-tunnel ctag-mapping dynamic

Use this command to enable or disable the dynamic customer VLAN tag learning mechanism for IPv4/IPv6 packets.

vlan-tunnel ctag-mapping dynamic { ipv4 | ipv6 } { enable | disable}

Syntax Description	
ipv4	Specifies IPv4 packets.
ipv6	Specifies IPv6 packets.
enable	Enables the VLAN tunnel dynamic customer VLAN tag learning mechanism.
disable	Disables the VLAN tunnel dynamic customer VLAN tag learning mechanism.

Default Disabled

Command Mode Global configuration

Usage Guideline Use this command to enable the dynamic customer VLAN tag learning mechanism. The mechanism learns the customer VLAN tag and source IP address mapping from incoming control packets. The learned customer VLAN tag mapping will be used for outgoing Layer 3 control packets. When a Layer 3 control packet is sent, and its destination IP is the same value as the source IP of dynamic learned customer VLAN tag mapping entry, then the control packet will be added to the matched customer VLAN tag.

If VLAN tunneling mode is disabled, the mechanism will not work even it is enabled.

Examples This example shows how to enable the VLAN tunnel dynamic customer VLAN tag learning mechanism for IPv4 packets.

```
Switch(config)# vlan-tunnel ctag-mapping dynamic ipv4 enable
```

Verify the settings by entering **show vlan-tunnel ctag-mapping dynamic state** command.

vlan-tunnel ctag-mapping static

Use this command to add a static customer VLAN tag mapping entry. Use the no form of the command to delete a static customer VLAN tag mapping entry.

vlan-tunnel ctag-mapping static {*A.B.C.D/M* | *X:X::X:X/M}* *C-VID*

no vlan-tunnel ctag-mapping static *{A.B.C.D/M* | *X:X::X:X/M}*

Syntax Description	
A.B.C.D/M	Specifies the destination IPv4 network address. A.B.C.D: IPv4 address M: IPv4 prefix length, maximum length is 32.
X:X::X:X/M	Specifies the destination IPv6 network address. X:X::X:X: IPv6 address M: IPv6 prefix length, maximum length is 128.
C-VID	The VLAN ID specified here refers to the inner-VID (i.e. customer VLA ID)

Default Not configured

Command Mode Global configuration

Usage Guideline Use this command to add a static customer VLAN tag mapping entry for the specified IP subnet.

Examples This example shows how to add a static customer VLAN tag mapping entry.

Using the following configuration, the *C-VID* 500 is used to add the out-going control packet which has destination IP equal to 10.90.90.1/24 subnet.

```
Switch(config)# vlan-tunnel ctag-mapping static 10.90.90.1/24 500
```

Verify the settings by entering **show vlan-tunnel ctag-mapping static** command.

vlan-tunnel ingress checking

Use this command to specify to drop the C-tagged packets that do not match any VLAN encapsulation pair or remarking pair. Use the no form of this command to allow the unmatched packet to be forwarded.

vlan-tunnel ingress-checking

no vlan-tunnel ingress-checking

Syntax None

Default Disabled

Command Mode Interface configuration (only available for a UNI port)

Usage Guideline If the receiving packet is tagged, the VLAN tunnel table (including VLAN encapsulation and VLAN remarking) is searched using the packet VLAN ID and the ingress port. If there is an entry missing, then the packet can optionally be dropped or have a SP VLAN (service provider VLAN) tag added based on the VLAN lookup tables (MAC, Subnet, Protocol, Port VLAN ID). When VLAN tunnel ingress filtering is enabled, the translation missed packets are dropped. If it has an SP VLAN tag added to the translation missed packet and forwared to the SP VLAN, it is referred to as VLAN tunnel ingress-checking disabled.

Examples This example shows how to enable the VLAN tunnel ingress-checking Ethernet eth3.1

```
Switch(config)#interface eth3.1
Switch(config-if)#vlan-tunnel ingress-checking
```

Verify the settings by entering **show vlan-tunnel** command.

vlan-tunnel interface-type

Use this command to configure an interface as NNI (Network-to Network) or UNI (User-to-Network).

vlan- tunnel interface-type { nni | uni }

Syntax Description	
nni | uni	Specifies the interface type for the interface (port channel or ethernet port). **nni** - Network to Network Interface. **uni** - User to Network Interface.

Default When a VLAN tunnel is enabled, all interface are set as a **nni** port.

Command Mode Interface configuration

Usage Guideline This command sets the interface type at the port used by the VLAN tunnel application.

uni - User to Network Interface.

nni - Networks to Network Interface.

Example This example shows how to set Ethernet eth3.1 NNI port.

```
Switch# configure terminal
Switch(config)#interface eth3.1
Switch(config-if)#vlan-tunnel interface-type nni
```

Verify the settings by entering **show vlan-tunnel** command.

vlan-tunnel remove-inner-tag

Use this command to strip off the packet's inner tag (C-TAG; should the packet have it) of the incoming packet. Use the no form of the command to keep the packet's inner tag.

vlan-tunnel remove-inner-tag

no vlan-tunnel remove-inner-tag

Syntax None

Default Disabled

Command Mode Interface configuration (only available for UNI ports only).

Usage Guideline The command is available only for a UNI port. If an incoming packet has an inner tag (C-TAG) and the packet is forwarded to a UNI port which is configured as remove-inner-tag enabled, then the packet's inner tag is removed.

Example This example shows how to enable the **vlan-tunnel remove-inner-tag** in Ethernet eth3.1

```
Switch(config)#interface eth3.1
Switch(config-if)#vlan-tunnel remove-inner-tag
```

Verify the settings by entering **show vlan-tunnel** command.

vlan-tunnel tpid

Use this command to specify the outer tag TPID at a Network-to-Network Interface (NNI) for the VLAN tunnel application.

vlan-tunnel tpid *TPID*

Syntax Description	
TPID	Specifies the TPID for the VLAN tag. The value is in hexadecimal form. Range is 0x0 to 0xFFFF.

Default 0x88A8

Command Mode Interface configuration (physical port and port channel interface only).

Usage Guideline This setting is only available for an NNI port in VLAN tunnel mode. The following shows the TPID usage for the NNI setting:

1. Packet transmitted at an NNI port.
    a. As a packet is transmitted from an NNI port for VLAN encapsulation, a TPID specified by the v**lan-tunnel tpid** command is used for the S tag (outer tag) TPID.
    b. As a packet is transmitted at an NNI port for VLAN remarking (replacement), a TPID specified by the **vlan-tunnel tpid** command is used for the VLAN tag TPID.
2. Packet received at an NNI port:
    a. As a packet is received at an NNI port, the TPID specified by the **vlan-tunnel tpid** command is used to identify whether or not the packet has an S tag (outer tag).

Example This example shows how to set outer TPID at eth3.12 to 0x9100.

```
Switch(config)#interface eth3.12
Switch(config-if)#vlan-tunnel tpid 0x9100
```

Verify the settings by entering the **show vlan-tunnel** command.

voice-vlan

Use the command to enable the voice VLAN function and to configure a VLAN as a voice VLAN. Use no form of this command to disable the voice VLAN function.

voice-vlan *VLAN-ID*

no voice-vlan

Syntax Description	
VLAN-ID	Specify the ID of the voice VLAN. The valid voice VLAN ID range is from 1 to 4094.

Default The voice VLAN state is disabled.

Command Mode Global configuration mode

Usage Guideline This command is used to enable the global voice VLAN function and to specify the voice VLAN on a switch. The switch has only one voice VLAN.

When voice VLAN is enabled, the switch will add a VLAN tag with the specified voice VLAN ID and the specified priority to the received untagged voice packets. The received packets are determined as voice packets if the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the switch.

The specified voice VLAN does not need to exist to apply the command.

Example The following example shows how to enable the voice VLAN function and configure VLAN 1000 as a voice VLAN.

```
Switch(config)#voice-vlan 1000
Switch(config)#end
Switch#
```

You can verify your settings by entering **show vlan voice-vlan** command.

voice-vlan cos

Use the command to configure the CoS priority for incoming voice VLAN traffic..

voice-vlan cos *COS-VALUE*

Syntax Description	
COS-VALUE	Specify the priority of voice VLAN. The available value is 0~7.

Default The default CoS priority is 5.

Command Mode Global configuration mode.

Usage Guideline The voice VLAN priority will be the priority associated with the voice VLAN traffic to distinguish the QoS of the voice traffic from data traffic.

Example The example shows how to configure the priority of the voice VLAN to be seven.

```
Switch(config)#voice-vlan cos 7
Switch(config)#end
Switch#
```

You can verify your settings by entering **show vlan voice-vlan** command.

voice-vlan oui

Use the command to add the user defined OUI of voice device. Use no form of this command to delete the user defined OUI of voice device.

voice-vlan oui MAC-ADDRESS MASK [**description** TEXT]

no voice-vlan oui MAC-ADDRESS **MASK**

Syntax Description

MAC-ADDRESS	Specify the OUI MAC address.
MASK	Specify the OUI MAC address mask.
description	(Optional) The description of the user defined OUI.
TEXT	(Optional) Specify the description of user defined OUI, an ASCII string from 1 to 32 characters.

Default The default OUI is listed in the following table.

OUI	Vendor
00:01:E3	Siemens
00:03:6B	Cisco
00:09:6E	Avaya
00:0F:E2	Huawei-3COM
00:60:B9	NEC/ Philips
00:D0:1E	Pingtel
00:E0:75	Veritel
00:E0:BB	3COM

Command Mode Global configuration mode.

Usage Guideline This command is used to add user defined OUI(s) for the voice VLAN. The OUI of voice VLAN is used to identify the voice traffic if voice VLAN is enabled.

If the source MAC addresses of received packets comply with the configured OUI addresses, the received packets are determined as voice packets.

The default OUI cannot be deleted.

Example This example shows how to add a user defined OUI of voice device.

```
Switch(config)#voice-vlan oui 01-02-03-04-05-06 ff-ff-ff-ff-ff-ff
Switch(config)#end
Switch#
```

You can verify your settings by **show vlan voice-vlan** oui command.

vrrp critical-ip

Use this command to configure the critical IP address. To remove the critical IP address using the no form of this command.

vrrp *VRID* **critical-ip** *IP-ADDRESS*

no vrrp *VRID* **critical-ip**

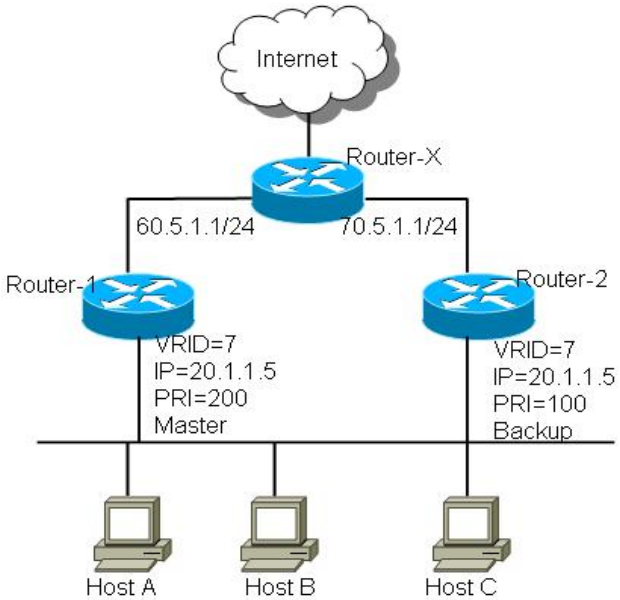
Syntax Description	
VRID	Specifies the Virtual router identifier, which is the number identifying the virtual router for which the critical IP address is being configured. The virtual router identifier is configured with the command **"vrrp ip" on page 917**. Range is from 1 to 255.
IP-ADDRESS	Specifies the IP address of the neighbor router that provide the most direct route to the Internet.

Default Not configured

Command Mode Interface configuration

Usage Guideline Referring to the figure below, Router-1 is the VRRP master router while Router-2 is the backup router for virtual IP 20.1.1.5. For the master router, the next hop router which provides access to the Interface is Router-X and the interface IP address on Router-X that connects to Router-1 is 60.5.1.1. IP address 60.5.1.1 is the critical IP address for the master router.

Configure the critical IP address on the master router and the master router will monitor the ARP cache of the critical IP address. Once the ARP cache of critical IP is gone from the ARP table, the master router will give up its master status.



Examples

The following example shows how to configure the critical-ip address 60.5.1.1 for virtual router 7 with priority 200 on interface vlan1.

```
Switch(config)#interface vlan1
Switch(config-if)#vrrp 7 ip 20.1.1.5
Switch(config-if)#vrrp 7 priority 200
Switch(config-if)#vrrp 7 critical-ip 60.5.1.1
```

The following example shows how to remove the critical-ip address for virtual router 7 on interface vlan1.

```
Switch(config)#interface vlan1
Switch(config-if)#no vrrp 7 critical-ip
```

vrrp ip

To enable the Virtual Router Redundancy Protocol (VRRP) on an interface and identify the IP address of the virtual router, use the **vrrp ip** command.

To disable VRRP on the interface and remove the IP address of the virtual router, use the no form of this command.

vrrp VRID ip *IP-ADDRESS*

no vrrp VRID

Syntax Description	
VRID	Specifies the virtual router identifier, which is the number that identifies the virtual router. Range is from 1 to 255.
IP-ADDRESS	Specifies the IP address of the virtual router.

Default Disabled

Command Mode Interface configuration

Usage Guideline The **vrrp ip** command activates VRRP on the configured interface. The IP address specified in the VRRP configuration is used as the address for the virtual router.

A master will be elected in a group of virtual routers which have the same virtual router identifier for forwarding the packets from the host that sends to this virtual router.

Examples The following example shows how to enable VRRP on vlan1. The virtual router identifier is 7, and 10.1.1.1 is the IP address of the virtual router.

```
Switch(config)#interface vlan1
Switch(config-if)#vrrp 7 ip 10.1.1.1
```

The following example shows how to remove the IP address of the virtual router and disable the VRRP on the interface.

```
Switch(config)#interface vlan1
Switch(config-if)#no vrrp 7
```

vrrp preempt

To configure the router to take over as the master virtual router for a Virtual Router Redundancy Protocol (VRRP) group, if it has higher priority than the current master virtual router, use the **vrrp preempt** command. To disable this function, use the no form of this command.

vrrp *VRID* **preempt**

no vrrp *VRID* **preempt**

Syntax Description	
VRID	Specifies the virtual router identifier, which is the number identifying the virtual router that preemption is being configured for. The virtual router identifier is configured with the command **"vrrp ip" on page 917**. Range is from 1 to 255.

Default Enabled

Command Mode Interface configuration

Usage Guideline A backup router will not attempt to preempt the master unless it has higher priority.

This command controls whether a higher priority backup router preempts a lower priority master.

By default, the router preempt mode is enabled on the router when it takes over as master router for the virtual router if, it has a higher priority than the current master router.

After using the no form of this command, the preempt mode changes to disabled, and the backup router will not attempt to preempt the master router even if it has a higher priority than the master router.

One exception is that the router, that is the virtual IP address owner, always preempts, regardless of the setting of this command.

Examples The following example shows how to configure the router to preempt the current master router when its priority of 200 is higher than that of the current master router.

```
Switch(config)#interface vlan1
Switch(config-if)#vrrp 7 preempt
Switch(config-if)#vrrp 7 priority 200
```

The following example shows how to configure the router to disable preempt of a virtual router.

```
Switch(config)#interface vlan1
Switch(config-if)#no vrrp 7 preempt
```

vrrp priority

To set the priority of the virtual router, use the **vrrp priority** command in VRRP interface configuration mode.

To restore the default priority value of the virtual router, use the no form of this command.

vrrp VRID priority *PRIORITY*

no vrrp VRID priority

Syntax Description	
VRID	Specifies the virtual router identifier, which is the number that identifies the virtual router fthat the priority is being configured for. The virtual router identifier is configured with the command **"vrrp ip" on page 917**. Range is from 1 to 255.
PRIORITY	Specifies the priority of the virtual router. Higher values equal higher priority. Range is from 1 to 254

Default *Priority*: 100

Command Mode Interface configuration

Usage Guideline Use this command to control which router becomes the master router. This command is ignored while the router is the virtual IP address owner.

The router with the highest priority will become the master, and other routers with lower priority will then become the backups for the virtual router. Each router should be configured with different priority values. If there is more than one router accidently configured to have the same highest priority, then one of them will become the master which depends on which one of them sends the advertisement packet out first. If the advertisement packets are sent out at the same time, the primary IP address (see Note 1) will be compared. The router with greater primary IP address becomes the master.

Note 1: the primary IP address is the interface IP address that is configured by the command **"ip address" on page 216**.

Examples The following example shows how to configure the router with a priority of 200.

```
Switch(config)#interface vlan1
Switch(config-if)#vrrp 7 priority 200
```

The following example shows how to restore the default priority of the virtual router.

```
Switch(config)#interface vlan1
Switch(config-if)#no vrrp 7 priority
```

vrrp shutdown

This command is to disable the VRRP of a VRID on an interface. Use the no form of the command to re-activate the VRRP.

vrrp *VRID* **shutdown**

no vrrp *VRID* **shutdown**

Syntax Description	
VRID	Specifies the virtual router identifier, the number identifying the virtual router that the shutdown is being configured for. The virtual router identifier is configured with the command **"vrrp ip" on page 917**. Range is from 1 to 255.

Default None

Command Mode Interface configuration

Usage Guideline When a VRRP VRID is being configured using the **vrrp VRID ip** command, the protocol will be fully operational. Using **vrrp shutdown** disables the protocol operation for one VRID of an interface.

Examples The following example shows how to disable one VRRP VRID 7 on interface vlan1 while retaining the VRRP VRID 8.

```
Switch(config)#interface vlan1
Switch(config-if)#vrrp 7 ip 20.1.1.1
Switch(config-if)#vrrp 7 shutdown
Switch(config-if)#
Switch(config-if)#vrrp 8 ip 20.1.1.2
Switch(config-if)#
```

The following example shows how to re-activate VRRP protocol on VRID 7 of interface vlan1.

```
Switch(config)#interface vlan1
Switch(config-if)#no vrrp 7 shutdown
```

vrrp timers advertise

This command configures the interval between successive advertisements by the master router. To restore the default value, use the no form of this command.

vrrp VRID timers advertise *INTERVAL*

no vrrp VRID timers advertise

Syntax Description	
VRID	Specifies the virtual router identifier, which is the number identifying the virtual router that the advertisement timing is being configured for. The virtual router identifier is configured with the command **"vrrp ip" on page 917**. Range is from 1 to 255.
INTERVAL	Time interval between successive advertisements by the master router. The unit of the interval is in seconds. Range is from 1 to 255 seconds.

Default *Interval*: 1 second

Command Mode Interface configuration

Usage Guideline The VRRP advertisements being sent by the master virtual router communicate the state and priority of the current master virtual router.

The **vrrp timers advertise** command configures the time between the advertisement packets and the time before other routers declare the master router to be down. All routers in a VRRP group must use the same timer values.

Examples The following example shows how to configure the router to send advertisements every 10 seconds.

```
Switch(config)#interface vlan1
Switch(config-if)#vrrp 7 timers advertise 10
```

The following example shows how to configure the advertisement interval to default.

```
Switch(config)#interface vlan1
Switch(config-if)#no vrrp 7 timers advertise
```

Acronym List

ACL	Access Control List
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Unit
CHAP	Challenge Handshake Authentication Protocol
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLI	Command-Line Interface
CLNS	Connection-Less Network Service
CoS	Class of Service
CPLD	Complex Programmable Logic Device
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Configuration Protocol
DM	Dense Mode (PIM)
DNS	Domain Name System
DoS	Denial of Service

dot1q	802.1Q
dot1x	802.1X
DRAM	Dynamic RAM
DVMRP	Distance Vector Multicast Routing Protocol
EAP	Extensible Authentication Protocol
FAT	File Allocation Table
FIB	Forwarding Information Base
FTP	File Transfer Protocol
GARP	General Attribute Registration Protocol
GBIC	Gigabit Interface Converter
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGMPv2	IGMP version 2
IGMPv3	IGMP version 3
IGRP	Interior Gateway Routing Protocol

ILMI	Integrated Local Management Interface
IP	Internet Protocol
IS-IS	Intermediate System-to-Intermediate System Intradomain Routing Protocol
ISO	International Organization of Standardization
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol data unit
LAN	Local Area Network
LAPB	Link Access Procedure, Balanced
LCP	Link Control Protocol
LLC	Logical Link Control
MAC	Media Access Control
MD5	Message Digest 5
MED	Multi-Exit Discriminator
MIB	Management Information Base
mroute	multicast route
mrouter	multicast router
MST	Multiple Spanning Tree (802.1s)

MSTCI	MST configuration identifier
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NetBIOS	Network Basic Input/Output System
NSAP	Network Service Access Point
NSF	Non-Stop Forwarding
NTP	Network Time Protocol
NVRAM	Non-Volatile RAM
OAM	Operation, Administration, and Maintenance
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PAE	Port Access Entity
PDU	Protocol Data Unit
PHY	Physical sublayer
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast Sparse Mode
PPP	Point-to-Point Protocol

QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RAM	Random-Access Memory
RIB	Routing Information Base
RMON	Remote Network Monitor
ROM	Read-Only Memory
RP	Route Processor
RSTP	Rapid Spanning Tree Protocol
RTP	Real-Time Transport Protocol
SM	Sparse Mode (PIM)