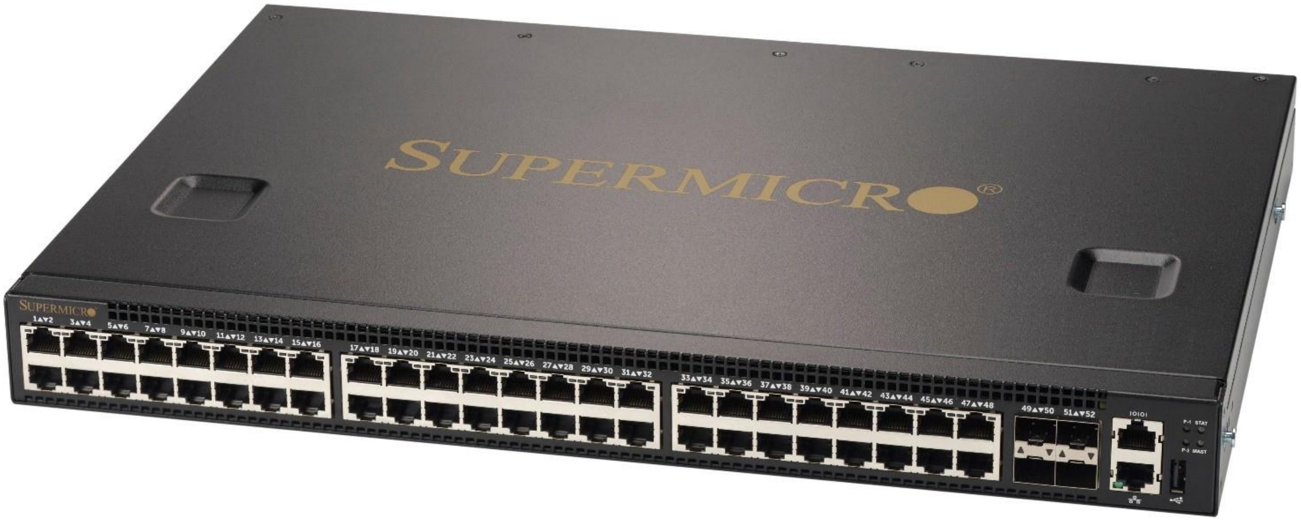
SSE-G3648B/SSE-G3648BR Switch
CLI User's Guide



Revision 1.1

The information in this USER'S GUIDE has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person organization of the updates. Please Note: For the most up-to-date version of this manual, please see our web site at www.supermicro.com.

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

DISCLAIMER OF WARRANTY ON SOFTWARE AND MATERIALS. You expressly acknowledge and agree that use of the Software and Materials is at your sole risk. FURTHERMORE, SUPER MICRO COMPUTER INC. DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE OR MATERIALS IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY SUPER MICRO COMPUTER INC. OR SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SHOULD THE SOFTWARE AND/OR MATERIALS PROVE DEFECTIVE, YOU (AND NOT SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICE, REPAIR, OR CORRECTION.

LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES INCLUDING NEGLIGENCE, SHALL SUPER MICRO COMPUTER INC. BE LIABLE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES THAT RESULT FROM THE USE OR INABILITY TO USE THE SOFTWARE OR MATERIALS, EVEN IF SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Super Micro's total liability for all claims will not exceed the price paid for the hardware product.

Manual Revision 1.0.1
Release Date: 1/15/2020

Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Document Revision History

Date	Revision	Description
09/17/2018	1.0	Initial document.
01/15/2020	1.0.1	Unique password update Notes for firmware upgrade
02/11/2020	1.0.2	Add "show transceiver", "onie bootmode", "ztp enable", and "reset-to-factory-default" to chapter 4

Contents

1 Introduction

1.1 Scope

The scope of this document is limited to SMIS release 2.0.0 and above. This document details all the Base CLI commands provided by the SMIS software. Commands that are not applicable for a specific hardware platform are indicated wherever necessary.

1.2 Document Conventions

- The syntax of the CLI command is given in **Courier New 10 bold .**
- Elements in (< >) indicate the field required as input along with a CLI command, for example, < integer (100-1000)>.
- Elements in square brackets ([]) indicate optional fields for a command.
- Text in {} refers to either or group for the tokens given inside separated by a | symbol.
- The CLI command usage is given in `Courier New 10 regular`.
- Outputs and messages for CLI commands are given in `Courier New 10 regular`.
- The No form of the command resets a particular configuration to its default value or revokes the effect. This is explicitly explained in the description of the commands for which it is applicable.
- Any action that can change the switch configuration, conditionals and requirements for a command and information associated with significant details and functionality of a command begin with the word **Note:** in bold.

1.3 Industry Standard CLI

CLI commands are focused on performing specific operations. In order to provide a consistent, composable user experience, the CLI commands of the protocols and solutions, have been modified to adhere to the Industry Standard CLI syntax. This enhancement is available for the code base using release after SMIS 2.0.0.

1.4 Key Conventions

1.4.1 Keyboard Shortcuts

- **Up Arrow / Down Arrow** - Displays the previously executed command.
- **Backspace / Ctrl + H** - Removes a single character.
- **TAB** - Completes a command without typing the full word.
- **Left Arrow / Right Arrow** - Traverses the current line.

1.4.2 Others

- **?** - helps to list the available command
- **Q** - exits and returns to the SMIS prompt
- **History** - displays the command history list

2 Command Line Interface

This section describes the configuration of Supermicro **SMIS** using the Command Line Interface.

The Command Line Interface (CLI) can be used to configure the Intelligent Switch Solution from a console attached to the serial port of the switch or from a remote terminal using TELNET.

The CLI supports a simple login authentication mechanism. The authentication is based on a user name and password provided by the user during login. The user "ADMIN" is created by default with an unique password. The unique password is printed on the label on the top of the switch along with the switch serial number and MAC address.

A new user can be created or an existing user can be deleted, and the own password or password of the other users can be modified, only if login as an ADMIN user.

> When **SMIS** is started, the user name and password has to be given at the login prompt to access the CLI shell:
> Supermicro Switch **`SMIS Login: ADMIN Password: *****`**
> `SMIS>`

The **user-exec** mode is now available to the user. CLI command modes provide a detailed description of the various modes available for SMIS.

The command prompt always displays the current mode, CLI commands need not be fully typed. The abbreviated forms of CLI commands are also accepted by the SMIS CLI. For example, commands like "show ip global config" can be typed as "sh ip gl co".

CLI commands are case insensitive.

CLI commands will be successful only if the dependencies are satisfied for a particular command that is issued. The general dependency is that the module specific commands are available only when the respective module is `‘enabled’`.

Appropriate error messages will be displayed, if the dependencies are not satisfied.

The Ethernet type of an interface is determined during System Startup. While configuring interface- specific parameters, its Ethernet type needs to be specified correctly. A fast ethernet interface cannot be configured as a gigabit-ethernet interface and vice-versa.

2.1 Context Sensitive Help

SMIS CLI framework offers context sensitive help; the user can type a question mark (?) anytime during a session to get help. The help can be invoked in several ways. It is not displayed as a whole and is available only for the specific token from where it is invoked.

Examples of possible scenarios are given below.

1. User keys in a character followed immediately by a question mark (?). This displays the current possible tokens without help string.

```
SMIS(config)# bo?

bootfile
```

2. User enters a keyword at the command prompt and enters a question mark (?) after hitting a space. This displays the next possible tokens along with the corresponding helpstring.

```
SMIS(config)# service ?

dhcp          DHCP related configuration

dhcp-relay    DHCP relay related configuration dhcp-server    DHCP server related configuration
timestamps    Timestamp configuration for logged messages
```

Some of the basic concepts implemented for the context sensitive help are:

- The next possible tokens are listed only in the lexical order and not in the order as available in the syntax or command structure.
- All possible tokens are listed along with the help string, even though the command is ambiguous. Any ambiguous command errors and value range errors are taken care only during the execution of the command.
- The help tokens provided within <> brackets denotes that the user should input values of specified format. For example, <string(32)> represents that the user should input a string of size varying from 1 to 32.
- The help tokens provided within () brackets denotes that the user should input only the values represented. For example, (1-4094) represents that the user should input value within the mentioned range alone.
- The format is directly provided as help token for some non-keyword such as IP address, IP mask , MAC address and so on. For example, aa:aa:aa:aa:aa:aa represents that a MAC address of this format should be provided.
- Only the most commonly used format is provided as help token for some non-keywords such as IPv6 address. But the command supports most of the valid formats. For example, AAAA::BBBB represents the IPv6 address, but the command will accept the format AAAA:B::BBBB.
- The help token <CR> along with help string explaining the operation of the command is displayed, if the command can be executed at that point (errors are handled only during the execution).

2.2 CLI command modes

The following table format lists the different CLI command modes. Depending on the CLI mode, your product prompt will be specific. This can be changed by the end user.

For example, if your product label is ABC and the command mode is GlobalConfiguration, the prompt display will be **`ABC (config)`**

Command Mode	Access Method	Prompt	Exit Method
User EXEC	This is the initial mode to start a session.	`Your Product>`	The logout method is used.
Privileged EXEC	The User EXEC mode command `enable` is used to enter the Privileged EXEC mode.	`Your Product#`	To return from the Privileged EXEC mode to User EXEC mode the `disable` command is used.
Global Configuration	The Privileged EXEC mode command `configure terminal` is used to enter the Global Configuration mode	`Your Product(config)#`	To exit to the Privileged EXEC mode the `end` command is used.
Interface Configuration	The Global Configuration mode command interface `<interface-type><interface-id>` is used to enter the Interface configuration mode	`Your Product(config-if)#`	To exit to the Global Configuration mode the `exit` command is used and to exit to the Privileged EXEC mode. the `end` command is used.
Interface Range Mode	The Global Configuration mode command interface range `( { <interface-type> <slot/port-port>} {vlan <vlan-id(1-4094)> -<vlan-id(2-4094)>})` is used to enter the Interface range mode.	`Your Product(config-if-range)#` Or `Your Product(config-if-range)#`	To exit to the Global Configuration mode the `exit` command is used to exit, and to the Privileged EXEC mode the `end` command is used.
Config-VLAN	The Global configuration mode command `vlan vlan- id` is used to enter the Config-VLAN mode.	`Your Product(config-vlan)#`	To exit to the Global Configuration mode the `exit` command is used, and to exit to the Privileged EXEC mode the `end` command is used
Line Configuration	The global configuration mode command `line` is used to enter the Line Configuration mode.	`Your Product(config-line)#`	To exit to the Global Configuration mode the `exit` command is used, and to exit to the Privileged EXEC mode the `end` command is used.

2.2.1 User EXEC Mode

After logging into the device, the user is automatically in the User EXEC mode. In general, the User EXEC commands are used to temporarily change terminal settings, perform basic tests and list system information.

2.2.2 Privileged EXEC Mode

Because many of the privileged commands set operating parameters, privileged access is password protected to prevent unauthorized use. The password is not displayed on the screen and is case sensitive. The Privileged EXEC mode prompt is the device name followed by the pound (#) sign.

2.2.3 Global Configuration Mode

Global Configuration commands apply to features that affect the system as a whole, rather to any specific interface.

2.2.4 Interface Configuration Mode

To enter into Interface configuration mode from the Global Configuration mode, **`interface`** `<interface-type><interface-id>` command is used. To exit to the global configuration mode the `exit` command is used and to exit to the privileged EXEC mode the `end` command is used.

2.2.5 Physical Interface Mode

The Physical Interface mode is used to perform interface specific operations. To return to the global configuration mode the `exit`command is used.

Port Channel Interface Mode

The Port Channel Interface mode is used to perform port-channel specific operations. To return to the global configuration mode the `exit`command is used.

VLAN Interface Mode

The VLAN Interface mode is used to perform L3-IPVLAN specific operations. To return to the global configuration mode the `exit`command is used.

Management Interface Mode

The management Interface mode is used to perform OOB interface specific operations. To return to the global configuration mode the `exit` command is used

2.2.6 Interface Range Mode

To enter into Interface range mode from the Global Configuration mode, `interface range ({ <interface-type> <slot/port-port>}{vlan <vlan-id(1-4094)> - <vlan-id(2-4094)>})` command is used. To exit to the global configuration mode the `exit` command is used and to exit to the privileged EXEC mode the `end` command is used.

2.2.7 Config-VLAN Mode

This mode is used to perform VLAN specific operations. To enter into Config-VLAN mode from the global configuration mode, `vlan vlan-id` command is used. To return to the global configuration mode the `exit` command is used.

2.2.8 Line Configuration Mode

Line configuration commands modify the operations of a terminal line. These commands are used to change terminal parameter settings line by line or range of lines. To enter into Line Configuration mode from the global configuration mode, `line` command is used. To exit to the Global Configuration mode the `exit` command is used and to exit to the Privileged EXEC mode the **end** command is used.

2.2.9 Protocol Specific Modes

The following are the specified protocol modes;

- VRRP Router Configuration Mode
- VRRP Interface Configuration Mode
- DHCP Pool Configuration Mode
- SNTP Configuration Mode
- MSTP Configuration mode
- DiffSrv ClassMap Configuration mode
- DiffSrv Policy-Map Configuration Mode
- ACL Standard Access List Configuration Mode
- ACL Extended Access List Configuration Mode
- ACL MAC Configuration Mode
- CEE-Map Configuration Mode

VRRP Router Configuration Mode

This mode is used for configuring the virtual router. To enter to this mode, the command router vrrp from the Global configuration mode is used. To exit to the Global Configuration mode the `exit` command is used and to exit to the Privileged EXEC mode the **end** command is used.

VRRP Interface Configuration Mode

VRRP interface config mode is used to configure VRRP interfaces. To enter into this mode, `interface Vlan <vlan id>` command from VRRP router config mode is used. To exit to the Virtual Router Configuration mode the `exit` command is used and to exit to the Privileged EXEC mode the **end** command is used.

DHCP Pool Configuration Mode

This mode is used to configure the network pool/host configurations of a subnet pool.

The Global configuration mode command `ip dhcp pool <integer(1-2147483647)>` creates a DHCP Server address pool and places the user in DHCP pool configuration mode. The prompt seen at this mode is `Your Product(dhcp-config)#`.

To return to the global configuration mode the exitcommand is used.

SNTP Configuration Mode

SNTP Configuration mode is used to configure SNTP parameters. To enter into this mode, `sntp` command from the Global Configuration mode is used. The prompt seen at this mode is `Your Product(config-sntp)#`. To exit to the Global Configuration mode the `exit` command is used, and to exit to the Privileged EXEC mode the **end** command is used.

MSTP Configuration mode

This mode is used to configure the MSTP specific parameters for the switch. The Global configuration mode command `spanning tree mst configuration` is used to enter the MSTP Configuration mode and. the prompt seen at this mode is `Your Product (config-mst)#`.

To return to the global configuration mode the `exit` command is used.

DiffSrv ClassMap Configuration mode

The class-map global configuration command creates a class map to be used for matching the packets to the class whose index is specified and to enter the class-map configuration mode The Global configuration mode command class-map <short(1-65535)>is used to enter the DiffSrv ClassMap Configuration mode and. the prompt seen at this mode is Your Product (config-cmap)#.

To return to the global configuration mode the exit command is used.

DiffSrv Policy-Map Configuration Mode

In the Policy-Map Configuration mode the user can create or modify a policy map.

The Global configuration mode command policy-map <short(1-65535)> is used to enter the DiffSrv Policy Map Configuration mode and the prompt seen at this mode is Your Product(config-pmap)#.

To return to the global configuration mode the exit command is used.

ACL Standard Access List Configuration Mode

Standard access lists create filters based on IP address and network mask only (L3 filters only).

The Global configuration mode command ip access-list standard<(1-1000) creates IP ACLs and is used to enter the ACL Standard Access List Configuration mode. The prompt seen at this mode is Your Product(config-std-nacl)#.

To return to the global configuration mode the exit command is used.

ACL Extended Access List Configuration Mode

The Extended Access lists enables to specify filters based on the type of protocol, range of TCP/UDP ports as well as IP address and network mask (Layer 4 filters).

The Global configuration mode command ip access-list extended<(1001-65535)> is used to enter the ACL Extended Access List Configuration mode and the prompt seen at this mode is Your Product(config-ext-nacl)#.

To return to the global configuration mode the exit command is used.

ACL MAC Configuration Mode

The MAC access-list global configuration command creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user.

The Global configuration mode command mac access-list extended<(1-65535)> is used to enter the ACL MAC Configuration mode and the prompt seen at this mode is Your Product(config-ext-macl)#.

To return to the global configuration mode the exit command is used.

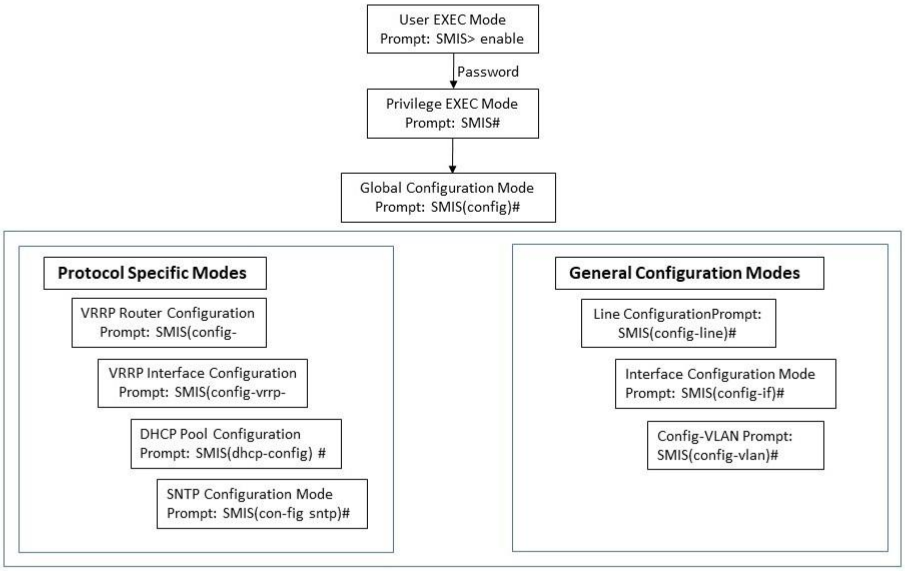
CEE-Map Configuration Mode

The CEE-Maps described the relationship between traffic priorities and priority-groups, and defined the settings of Priority-based Flow Control (PFC), and bandwidth allocation, to meet the requirement of Data

Center Bridging (DCB), conform to the CEE version.

The CEE-Maps will be associated with ports. If a port associated with a particular CEE-Map, then the port is ready to start a DCBX negotiation with its link partner, to achieve a converged Ethernet channel.

Global configuration mode command `cee-map <cee-map-id>` is used to create/enter the CEE-Map to change its settings, the `exit` command is used to return to the Global configuration mode. No form of this command to delete the CEE-Map.



3 System Commands

The System Commands describes the commands used to manage access permissions, mode access and terminal configurations on ISS.

The list of CLI commands for the configuration of System commands is as follows:

- help
- clear screen
- Enable
- Disable
- configure terminal
- configure
- run script
- listuser
- lock
- username

- enable password
- line
- alias - replacement string
- alias – interface | exec | configure
- access-list provision mode
- access-list commit
- exec-timeout
- logout
- end
- Exit
- show privilege
- show line
- show aliases
- show users
- show history
- password validate char
- password validate uppercase
- password validate lowercase
- password validate numbers
- password validate symbols
- set minimum password length
- show password validate rules
- show minimum password length
- password max-life-time
- show password max-life-time
- set cli pagination
- coredump
- show tech-support
- show meminfo

help

Command Objective This command displays a brief description for the given command. To display help description for commands with more than one word, do not provide any space between the words.

Syntax **help [command]**

Mode All Modes

Example

```
Your Product# help enable
```

The `Configure Terminal` command must be executed as:

```
Your Product# help configureterminal
```

clear screen

Command Objective This commandclears all the contents from the screen.

Syntax **clear screen**

Mode All Modes

Example `Your Product# clear screen`

enable

Command Objective This command enters into default level privileged mode. If required, the user can specify the privilege level by enabling level with a password (login password) protection to avoid unauthorized user.

Syntax **enable [<0-15> Enable Level]**

Parameter Description `<0-15> Enable level` sets the privilege level to enter the system. This value ranges between 0 and 15. Users with Privilege Level 0 can access only the following commands:

- Enable
- Disable
- Exit
- Help
- logout

Notes:

- This is the most restricted level.
- Users with Privilege Level 1 can access all user-level commands with the `SMIS> prompt`.
- The system allows configuring additional privilege levels (from level 2 to 14) to meet the needs of the users while protecting the system from unauthorized access. Users with Privilege Level 15 can access all commands. It is the least restricted level.

Mode User EXEC Mode

Default Enable level - 15

Example `Your Product# enable 15`

Related Command(s)

- `disable` - Turns off privileged commands
- `enable password` - Modifies enable password parameters

disable

Command Objective This command turns off privileged commands. This value ranges between 0 and 15. This value should be lesser than the privilege level value given in the enable command.

Syntax **disable [<0-15> Privilege level to go to]**

Mode User EXEC Mode

Example

```
Your Product# disable 1
```

Related Command(s) `enable` – Enters to privileged EXEC mode.

configure terminal

Command Objective This command enters to Global Configuration Mode which allows the user to execute all the commands that supports global configuration mode.

Syntax **configure terminal**

Mode Privileged EXEC Mode

Example

```
Your Product# configure terminal

Your Product (config)#
```

Related Command(s)

- `end` - Exits from Configuration mode and enters Privileged Configuration mode
- `exit` - Exits the current mode and reverts to the mode used prior to the current mode

configure

Command Objective This command enters the configuration mode. Configuration from memory or network is not supported, when entered into the configuration mode using this command

Note: This command is a complete standardized implementation of the existing command and operates similar to that of the command configure terminal

Syntax **configure**

Mode Privileged EXEC Mode

Example

```
Your Product# configure
```

Related Command(s)

- `end` - Exits from Current mode and enters Privileged EXEC mode
- `exit` - Exits the current mode and reverts to the mode used prior to the current mode.

run script

Command Objective This command runs CLI commands from the specified script file.

Syntax **run script [flash: | slot0: | volatile:] <script file> [<output file>]**

Parameter Description

`flash: | slot0: | volatile:` - Specifies the source of the script file.

- `Flash`- The script file is read from the Flash memory.
- `slot0` - The script file is read from the PCMCIA card or CompactFlash memory.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported

- `volatile` - The script file is read from the volatile memory. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
- `<script file>`- Specifies the script file to be executed
- `<output file>`- Specifies the output file

Mode Privileged EXEC Mode.

Example

```
Your Product# run script flash sample.js
```

listuser

Command Objective This command lists all the default and newly created users, along with their permissible mode.

Syntax **listuser**

Mode Privileged EXEC Mode

Example

```
Your Product# listuser
```

USER MODE ADMIN /

Guest /

Related Command(s) `show users` - Displays information about terminal lines.

lock

Command Objective This command locks the CLI console. It allows the user/system administrator to lock the console to prevent unauthorized users from gaining access to the CLI command shell. Enter the login password to release the console lock and access the CLI command shell.

Syntax **lock**

Mode Privileged EXEC Mode

Example

```
Your Product# lock
```

username

Command Objective This command creates a user and sets the enable password for that user with the privilege level.

The no form of the command deletes a user and disables the enable password for that user.

Syntax **username <user-name> [password <passwd>] [privilege<1-15>] [confirm-password <passwd>] [admin]**

no username < user-name >

Parmeter Description

- **<user-name>** - Specifies the login user name to be created
- **password <passwd>** – Specifies the password to be entered by the user to login to the system, and password encryption to be used. The size password entered must be a minimum of 8 and maximum of 20 characters containing at least one uppercase, one lowercase, one number and one special character.
- **privilege <1-15>** - Applies restriction to the user for accessing the CLI commands. This values ranges between 1 and 15. For example, a user ID configured with privilege level as four can access only the commands having privilege ID lesser than or equal to four.
- **confirm-password <passwd>** - Enter the password again to confirm it.
- **admin** - Set the user ID as the administrator.

Mode Global Configuration Mode

Notes:

- Privledge ID is set as zero for all the show commands and is set as 15 for all the configuration commands, in the def files. That is, root users can access all the commands and other users can access only the show commands. Users can change the privilege IDs of the commands in the def file to customize and segregate the commands as per the needs.
- If the user "ADMIN" is created as admin user, the password policy is skipped for checking. The default password must be "ADMIN".
- If the switch is reset to factory default, the user “ADMIN” is restored and the default password is the unique password printed on the label on the top of the switch along

with the switch serial number and MAC address.

- If user already exists, the administrator user can re-assign the password, privilege and admin for user.

Examples

- `Your Product (config)# username products password Prod@1234 privilege 15 confirm-password Prod@1234`

  Note: The user products are created with the privilege level 15. Hence, the user will be visible to view all the commands.

- `Your Product (config)# username support admin`

  Note: The user support is created with the the privilege level 15 and the default password "Smci123#". If not an admin user, the user support is created with privilege level is 1 and the default password "Smis123#".

- `Your Product (config)# username support password Supp@123 privilege 1 confirm-password Supp@123`

  Note: The user support is created with the privilege level 1. Hence, the user will be visible to view only the below commands:

- `Show` - Show commands related to all the features.
- `Enable` - Enables the privilege level.
- `Disable` - Disables the privilege level.

- `Exit`
- `Logout`
- `Clear`
- `Debug`
- `No Debug`

Related Command(s)

- `enable password` - Modifies enable password parameters
- `enable` – Enters to privileged EXEC mode
- `lisuser` – Lists all the users

enable password

Command Objective This command modifies enable password parameters.

The no form of the command disables/enable password parameters.

Syntax **enable password [level (1-15)] <LINE 'enable' password>**

no enable password [level (1-15)]

Parameter Description

- **level(1-15)** – This represents the privilege level for which the password is to be set. The level ranges from 1 to 15.

- **<LINE 'enable' password>** - Represents the password to be given.

Note: The password should follow the password configuration conventions, where it should contain at least one uppercase, one lowercase, one number and one special character.

Mode Global Configuration Mode

Example `Your Product (config)# enable password level 1 Ad@123`

Related Command(s)

- `username` - Creates a user and sets the password for that user with the privilege level
- `enable` - Enters to privileged EXEC mode

line

Command Objective This command identifies a specific line for configuration and enters the line configuration mode and allows the user to execute all the commands that supports line configuration mode.

Syntax **line {console | vty | <line-number(0-16)>}[<ending-line- number(3-16)>]**

Parameter Description

- **console** - Specifies the line for configuration as `console`, and enters the console line configuration mode
- **vty** - Specifies the line for configuration as Virtual terminal line
- **<line-number(0-16)>** - Specifies the ID of a specific telnet session or initial telnet session in a configured series of telnet sessions. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported
- **<ending-line-number(3-16)>** - Specifies the ID of the last telnet session in a configured series of telnet sessions. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported

Mode Global Configuration Mode

Example

```
Your Product (config)# line console
Your Product (config-line)#
```

Related Command(s)

- `end` - Exits from Configuration mode and enters Privileged Exec mode
- `exit` - Exits the current mode and reverts to the mode used prior to the current mode
- `show line` - TTY line information

alias - replacementstring

Command Objective This command replaces the given token by the given string.

The no form of the command removes the alias created for the given string.

Syntax **alias <replacement string> <token to be replaced>no alias <alias>**

Parameter Description

- `<replacement string>/ <alias>` - Specifies the string for which a replacementis needed.
- `<token to be replaced>` - Specifies an abbreviated/ short form of the replacement string

Mode Global Configuration Mode

Example

```
Your Product# alias products pdt
```

Related Command(s) `show aliases` - Displays the aliases

alias – interface | exec | configure

Command Objective This command replaces the given token / command with the given string. This command is a standardized implementation of the existing command. It operates similar to that of the command alias-replacement, except that it allows the user to type a command with multiple tokens without quotes.

Syntax **alias {interface | exec | configure} <alias-name> { command<max 10 tokens> | token }**

Paramter Description

- **interface** - Specifies the commands executed in interface configuration mode. This feature has been included to adhere to the IndustryStandard
- **CLI syntax -** This feature is currently notsupported.
- **exec -** Specifies the commands executed in privileged EXEC / user EXEC mode. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported
- **configure -** Specifies the commands executed in configuration mode (That is, global, line, profile, vlan, switch and protocol specific configuration modes). This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported
- **<alias-name> -** Specifies the alternate name to be used for the command or token.
- **command <max 10 tokens>** - Specifies the commandand token values for which alias name should be configured.
- **token -** Specifies the token for which alias name should be configured.

Mode Global Configuration Mode

Note: The alias name can be set only for the commands, having equal to or less than 10 tokens.

Example

```
Your Product (config)# alias ln line
```

Related Command(s) `show aliases` - Displays the aliases

access-list provision mode

Command Objective This command removes the limit on number of unicast MAC entries indications to control.

Syntax **access-list provision mode { consolidated | immediate }**

Parameter Description

- `consolidated` - Configures the provision mode as consolidated.
- `immediate`- Configures the provision mode as immediate.

Mode Global Configuration Mode

Default immediate

Example

```
Your Product (config)# access-list provision mode consolidated
```

access-list commit

Command Objective This command triggers provisioning of active filter rules to hardware based on configured priority. This command is applicable only when provision mode is consolidated. Traffic flow would be impacted when filter-rules are reprogrammed to hardware.

Syntax **access-list commit**

Mode Global Configuration Mode

Example

```
Your Product# access-list commit
```

exec-timeout

Command Objective This command sets a time (in seconds) for EXEC line disconnection. This value ranges between 1 and 18000 seconds.

The no form of this command resets the EXEC timeout to its default value.

Syntax **exec-timeout <integer (1-18000)>**
no exec-timeout

Mode Line Configuration Mode

Default integer - 1800 seconds

Example

```
Your Product (config-line)# exec-timeout 100
```

Related Command(s) `line` - Configures a console/virtual terminal line

logout

Command Objective This command exits from Privileged EXEC/ User EXEC mode to ISS Login Prompt in case of console session. In case of a telnet session, this command terminates the session.

Syntax **logout**

Mode User EXEC Mode

Examples

- `Your Product# logout`
- `Your Product login:`

end

Command Objective This command exits from the current mode to the Privileged EXEC mode.

Syntax **end**

Mode All modes

Example `Your Product# end`

Related Command(s) `exit` – Exits the current mode and reverts to the mode used prior to the current mode.

Exit

Command Objective This command exits the current mode and reverts to the mode used prior to the current mode

Syntax **exit**

Mode All modes

Example `Your Product# exit`

Related Command(s) `end` - Exits from Configuration mode to the Privileged EXEC mode

show privilege

Command Objective This command shows the current user privilege level.

Syntax **show privilege**

Mode Privileged EXEC Mode

Example

```
Your Product# show privilege
Current privilege level is 15
```

Related Command(s) `enable` – Enters to Privileged EXEC Mode.

show line

Command Objective This command displays TTY line information such as EXEC timeout.

Syntax **show line {console | vty <line>}**

Mode Privileged EXEC Mode

Example

```
Your Product# show line console
Current Session Timeout (in secs) = 1800
```

Related Command(s)

- `line` - Configures a console/virtual terminal line
- `exec-timeout` – Sets a time (in seconds) for EXEC line disconnection.
- `clear line vty`- Clears the console or virtual terminal line to an idle state

show aliases

Command Objective This command displays all the aliases.

Syntax **show aliases**

Mode

Example

```
Your Product# show aliases
show -> sh privilege -> pr
```

Related Command(s) `alias-replacement string` - Replaces the given token by the given string

show users

Command Objective This command displays the information about the current user.

Syntax show users

Mode Privileged EXEC Mode

Example

```
Your Product# show users
Line           User            Peer-Address
0 con          ADMIN            Local Peer
```

Related Command(s) `Listuser` – Lists all valid users, along with their permissible mode

show history

Command Objective This command displays a list of recently executed commands.

Syntax **show history**

Mode Privileged EXEC Mode

Example

- `Your Product# show history`
- `show ip int`
- `show debug-logging`
- `show users`
- `show line`
- `show line console`
- `c s`
- `show aliases`
- `show privilege`
- `listuser`
- `show users`
- `show history`

password validate char

Command Objective This command configure the type of characters to be considered for password validation rules and takes values as bit mask.

Syntax **password validate char [lowercase] [uppercase] [numbers] [symbols]**

Parameter Description

- `lowercase` - Sets lowercase flag for password validation.
- `uppercase` - Sets uppercase flag for password validation.
- `numbers` – Sets numbers flag for password validation.
- `symbols` – Sets symbols flag for password validation.

Mode Global Configuration Mode

Default All flags are enabled

Example `Your Product (config)# password validate char lowercase`

RelatedCommand(s) `show password validate rules` - Displays the password validation rules.

password validate uppercase

Command Objective This command configures the minimum number of upper case characters that are to be present in the password. If the given password has less than the configured number of upper case characters, it will not be allowed. This value ranges between 0 and 20.

Syntax **password validate uppercase [<count(0-20)>]**

Mode Global Configuration Mode

Default Value 1

Example `Your Product (config) # password validate uppercase 1`

Related Command(s) `show password validate rules` – Displays the password validation rules.

password validate lowercase

Command Objective This command configures the minimum number of lower case characters that are to be present in the password. If the given password has less than the configured number of lower case characters, it will not be allowed. This value ranges between 0 and 20.

Syntax **password validate lowercase [<count(0-20)>]**

Mode Global Configuration Mode

Default Value 1

Example `Your Product (config) # password validate lowercase 1`

Related Command(s) `show password validate rules` – Displays the password validation rules.

password validate numbers

Command Objective This command configures the minimum numerical characters to be present in the password. If the given password has less than the configured number of numerical characters, it will not be allowed This value ranges between 0 and 20.

Syntax **password validate numbers [<count(0-20)>]**

Mode Global Configuration Mode

Default Value 1

Example `Your Product (config) # password validate numbers 1`

RelatedCommand(s) `show password validate rules`- Displays the password validation rules.

password validate symbols

Command Objective This command configures the minimum special character to be present in the password. If the given password has less than the configured number of symbols, it will not be allowed. This value ranges between 0 and 20.

Syntax **password validate symbols [<count(0-20)>]**

Mode Global Configuration Mode

Default Value 1

Example `Your Product (config) # password validate symbols 1`

Related Command(s) `show password validate rules` - Displays the password validation rules.

set minimum password length

Command Objective This command configures minimum password length. If the given password has less than the configured password length, it will not be allowed This value ranges between 8 and 20.

Syntax **set minimum password length <minimum-len>**

Mode Global Configuration Mode

Default Value 8

Example `Your Product (config) # set minimum password length 8`

Related Command(s) `show minimum password length` - Displays minimum password length

show password validate rules

Command Objective This command displays the password validation rules.

Syntax **show password validate rules**

Mode Privileged EXEC Mode

Example

```
Your Product# show password validate rules
Password Validation Mask : a
```

```
Min Lowercase char count : 2
Min Uppercase char count : 2
Min  Numeric  char  count  :  2
Min Symbol char count     : 2
```

Related Command(s)

- `password validate uppercase` - Sets the minimum uppercase characters to be present in the password
- `password validate lowercase` - Sets the minimum lowercase characters to be present in the password
- `password validate numbers` - Sets the minimum numerical characters to be present in the password
- `password validate symbols` - Sets the minimum special character to be present in the password

show minimum passwordlength

Command Objective This command displays minimum password length.

Syntax **show minimum password length**

Mode Privileged EXEC Mode

Example

```
Your Product# show minimum password length

Minimum Password length : 8
```

Related Command(s) `set minimum password length` – Configures minimum password length

password max-life-time

Command Objective This command configures the time after which the user password has to be expired in days. This value ranges between 0 and 366 days. The default value of password-max-life-time is 0 days, indicates the password does not expire.

Syntax **password max-life-time [<days (0-366)>]**

Mode Global Configuration Mode

Default Value 0 days

Example

```
Your Product (config) # password max-life-time 1
```

Related Command(s) `show password max-life-time` – Displays the password expiry time

show password max-life-time

Command Objective This command displays the password expiry time.

Syntax **show password max-life-time**

Example

```
Your Product# show password max-life-time
Password Max Life Time: 365
```

Related Command(s) `password max-life-time` – Configures the max life time after which the password has to be expired

set cli pagination

Command Objective This command enables/disables pagination.

Syntax **set cli pagination {on | off}**

Mode Global Configuration Mod

Example

```
Your Product(config)# set cli pagination off
Your Product(config)#
```

Related Command(s) Any command which will display long content on the screen, with pagination enabled, the `--More--` prompt will appear and pause listing when certain lines are displayed, users can press any key to resume listing of the content.

coredump

Command Objective Copies coredump to usb flash disk or remote location.

Syntax **coredump {tftp://ip-address/filename | sftp://<user-name>:<pass-word>@ip-address/filename | usb:filename }**

Parameter Description

- `tftp://ip-address/filename` - Configures the TFTP details for taking back up of system logs in TFTP server.
  - `ip-address` - the IP address or host name of the TFTP server.
  - `filename` - The name of the file in which the system logs should be stored. Filenames and directory names are case sensitive
- `sftp://<user-name>:<pass-word>@ip-address/filename` - Configures the SFTP details for taking back up of system logs in SFTP server.
  - `user-name` - The user name of remote host or server.
  - `pass-word` – The password for the corresponding user name of remote host or server.

- `ip-address`- The IP address or host name of the server.
- `filename` - The name of the file in which the system logs should be stored. Filenames and directory names are case sensitive

Mode All Modes

Example

```
Your Product# coredump tftp://10.0.0.10/test
```

show tech-support

Command Objective Displays details useful for technical support troubleshooting.

Syntax **show tech-support**

Mode All Modes

Example Your Product# show tech-support

show meminfo

Command Objective Displays memory information.

Syntax **show meminfo**

Mode All Modes

Example

```
Your Product# show meminfo
```

4 System Features

SMIS offers a rich set of system features to a user, such as login services, copying / writing facilities, duplex / negotiation support, and many other capabilities. Some features have special hardware requirements and others have special design considerations.

CFA (Common Forwarding Agent) is a proprietary module, which acts as a common forwarder of packets between the Network Protocol Module(s), the Data-Link Layer Protocol Layer Module(s) and the Device Drivers. CFA provides central management of the generic parameters of all the interfaces in the system.

The list of CLI commands for the configuration of system features is as follows:

- default mode
- default restore-file
- ip address

- Switchport
- ip address - rarp/dhcp
- login authentication
- login authentication-default
- authorized-manager ip-source
- ip http port
- set ip http
- mtu frame size
- system mtu
- bridge port-type
- system-specific port-id
- set custom-param
- mac-addr
- snmp trap link-status
- Write
- copy
- copy startup-config
- copy running-config startup-config
- copy logs
- firmware upgrade
- copy - file
- clock set
- erase
- cli console
- flowcontrol
- tunnel mode
- tunnel checksum
- tunnel path-mtu-discovery
- tunnel udlr
- shutdown - physical/VLAN/port-channel/tunnel Interface
- debug interface
- debug-logging
- incremental-save
- auto-save trigger
- set switch maximum - threshold
- set switch temperature -threshold
- set switch power -threshold
- mac-learn-rate
- system contact
- system location
- clear interfaces - counters
- clear counters

- show ip interface
- show authorized-managers
- show interfaces
- show interfaces - counters
- show system-specific port-id
- show custom-param
- show interface mtu
- show interface bridge port-type
- show nvram
- show env
- show system information
- show flow-control
- show debug-logging
- show debugging
- show clock
- show running-config
- show http server status
- show system acknowledgement
- show mac-learn-rate
- port-isolation in_vlan_ID
- show port-isolation
- private-vlan mapping
- audit-logging
- audit-logging filename
- audit-logging filesize
- audit-logging
- reset show
- config log
- hol blocking prevention
- internal-lan
- show internal-lan
- show iftype protocol deny table
- clear line vty
- tunnel hop-limit
- login block-for
- audit-logging logsize-threshold
- feature telnet
- show telnet server
- show audit
- set http authentication-scheme
- set http redirection enable
- http redirect

- show http authentication-scheme
- show http redirection
- ENTITY MIB
- set entity physical-index
- show entity logical
- show entity physical
- show entity lp-mapping
- show entity alias-mapping
- show entity phy-containment
- set hitless-restart enable
- speed
- automatic-port-create
- port-type providerInstancePort
- sleep
- rate-limit pause
- cpu controlled learning
- traffic-separation control
- mdix auto
- set port
- config-restore
- set switch-name
- packet receive index
- packet send index port
- packet send index value
- show packet send index
- show packet receive index
- set mirroring
- default exec-timeout
- ip unnumbered
- clear http server statistics
- show license
- install license
- uninstall license
- copy debug-files

default mode

Command Objective This command configures the mode by which the default interface gets its IP address. This configuration takes effect only on switch restart.

Syntax **default mode { manual | dynamic }**

Parameter Description Assigns static IP address to the default interface. The IP address and IP mask configured by user are assigned to the default interface.

- `dynamic` – Assigns dynamic IP address to the default interface. That is, IP address provided by the server in the network is assigned to the default interface on switch reboot. The IP address is fetched through the dynamic IP address configuration protocols such as DHCP client, RARP client, and BOOTP client.

Mode Global Configuration Mode

Default manual

Example

```
Your Product(config)# default mode dynamic
```

Related Command(s)

- `show nvram` – Displays the current information stored in the NVRAM
- `default ip address allocation protocol` - Configures the protocol by which the default interface acquires its IP address
- `default ip address` - Configures the IP address and subnet mask for the default interface.
- `ip address -rarp/dhcp` – Configures the current VLAN / OOB interface to dynamically acquire an IP address from the RARP / DHCP server. The no form of the command resets the IP address for the interface to its default value.

default restore-file

Command Objective This command configures the path of the default restoration file from which the configuration should be restored in the flash when the system is restarted.

Syntax **default restore-file <filename>**

Mode Global Configuration Mode

Default `smis.conf`

Example

```
Your Product(config)# default restore-file restore.conf
```

Related Command(s) `show nvram` – Displays the current information stored in the NVRAM

ip address

Command Objective This command sets the IP address for an interface.

The no form of the command resets the IP address of the interface to its default value.

Syntax **ip address <ip-address> <subnet-mask> [secondary]**

no ip address [<ip_addr>]

Parameter Description

- `<ip-address>` - Sets the IP address for an interface. If the network in which the switch is implemented contains a server such as DHCP server, dynamically allocating IP address, the configured IP address should not be within the range of the addresses that will be allocated by the server to the other switches. This precaution avoids creation of IP address conflicts between the switches.
- `<subnet-mask>` – Sets the subnet mask for the configured IP address.

  Notes:

  - The configured subnet mask should be in the same subnet of the network in which the switch is placed.
  - The parameters ip-address and subnet-mask are used implicitly in BCM Target.
- `secondary` – Sets the configured IP address as an additional IP address for the interface (that is, the configured address is used as secondary address instead of primary address). The configuration of this feature is not supported on management interface.

Mode Interface Configuration Mode

This command is applicable in VLAN Interface Mode/OOB Interface Mode.

Default

- IP address specified in NVRAM is taken as default for the default VLAN identifier.
- IP address is assigned as 0.0.0.0 and subnet mask as 255.255.255.255 for other interfaces.
- The interface should be shutdown before executing this command.
- If the IP address of the interface to which you are connected is modified, then the connection to the switch will be lost.

Example

```
Your Product(config-if)# ip address 10.0.0.3 255.255.255.0 secondary
```

Related Command(s)

- `show nvram` - Displays the current information stored in the NVRAM.
- `show ip interface` - Displays the IP interface configuration for all interfaces available in the

switch.

- `shutdown – physical/VLAN/port-channel/tunnel Interface` - Disables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.

switchport

Command Objective This command configures the port as switch port. Only switch port Related Command are made available for the interface, when the port is configured as switch port.

The no form of the command resets the port as router port. Only router port Related Command are made available for the interface, when the port is configured as router port.

Syntax **switchport**

no switchport

Mode Interface Configuration Mode

Default `switchport`

Note: The interface should be shutdown before executing this command.

Example

```
Your Product(config-if)# switchport
```

Related Command(s)

- `release –` Releases, on the specified interface, the DHCP lease obtained for an IP address from a DHCP server.
- `renew`- Renews the DHCP lease for the interface specified.
- `ip dhcp relay circuit-id`– Configures circuit ID value for an interface.
- `ip dhcp relay remote-id`– Configures remote ID value for an interface.
- `show ip interface` - Displays the IP interface configuration for all interfaces available in the switch.
- `switchport filtering-utility-criteria` - Creates filtering utility criteria for the port.
- `switchport pvid` - Configures the PVID on the specified port.
- `switchport acceptable-frame-type` - Configures the type of VLAN dependent BPDU frames such as GMRP BPDU, that the port should accept during the VLAN membership configuration.
- `switchport ingress-filter` - Enables ingress filtering feature on the port.

- `switchport map protocols-`group - Maps the configured protocol group to a particular VLAN ID for an interface.
- `switchport priority default` - Configures the default ingress user priority for a port.
- `switchport mode` - Configures the mode of operation for a switch port.
- `switchport protected`- Enables switchport protection feature for a port.

ip address - rarp/dhcp

Command Objective This command configures the current VLAN / OOB interface to dynamically acquire an IP address from the RARP / DHCP server.

The no form of the command resets the IP address for the interface to its default value.

Syntax

ip address { dhcp | rarp}[client-id { FastEthernet | GigabitEthernet | Port-channel | Vlan } <interface_list>] [hostname <host_name>]

no ip address

Parameter Description

- `dhcp` – Allows the client device to obtain configuration parameters such as network address, from the DHCP server.
- `rarp` – Allows the client device to dynamically find its IP address from RARP server, when it has only its hardware address such as MACaddress.
- `client-id` – Sets the client identifier that specifies the interface type and hexadecimal MAC address of the specified interface. The various interface types that can be specified are:
  - `FastEthernet` - Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
  - `GigabitEthernet` - A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `Port-channel` - Logical interface that represents an aggregator which contains several ports aggregated together.
  - `Vlan` - Logical interface that specifies a group of hosts which can communicate with each other as in same broadcast domain.
- `<interface list>` - Sets the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel and VLAN. Only VLAN or port-channel ID is provided, for interface types VLAN and port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3. Feature not supported - This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
  - `hostname` – Sets the name of the host from which the IP address is to be acquired dynamically. Feature not supported - This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Interface Configuration Mode (VLAN)

Default dhcp

Example

```
Your Product(config-if)# ip address dhcp
```

Related Command(s)

- `show ip dhcp client stats` - Displays the DHCP client statistics information for interfaces that are configured to acquire IP address dynamically from the DHCP server.
- `release` - Releases, on the specified interface, the DHCP lease obtained for an IP address from a DHCP server.
- `renew` - Renews the DHCP lease for the interface specified

login authentication

Command Objective This command configures the authentication method for user logins for accessing the GUI to manage the switch. Few network routers and other network equipment allows access to a server or a managing computer to determine if the user attempting to log in has the proper rights or is in the user database.

The no form of the command resets the authentication method for user logins to its default values. Changing login authentication from default to another value may disconnect the telnet session.

Syntax

login authentication [{radius | tacacs }] [local]

no login authentication

Parameter Description

- `Radius` - Sets the RADIUS server to be used as an authentication server. Enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.
- `tacacs` - Sets the TACACS server to be used as an authentication server. Communicates with the authentication server commonly used innetworks.
- `local` - Sets locals authentication. The user identification, authentication, and authorization method is chosen by the local system administration and does not necessarily comply with any other profiles.

Mode Global Configuration Mode

Default Local

Example

```
Your Product(config)# login authentication radius
```

Related Command(s)

- `username` - Creates a user and sets the enable password for that user with the privilege level

- `no enable password`- Deletes a user and disables enable password parameters
- `show system information` - Displays system information

login authentication-default

Command Objective This command configures the authentication method for user logins for accessing the GUI to manage the switch. Few network routers and other network equipment allows access to a server or a managing computer to determine if the user attempting to log in has the proper rights or is in the user database.

Notes: Changing login authentication from default to another value may disconnect the telnet session.

The no form of the command resets the authentication method for user logins to its default values.

Note: This command is a standardized implementation of the existing command. It operates similar to that of the `command login authentication`.

Syntax

login authentication { default | <list-name> }

no login authentication { default | <list-name> }

Parameter Description

- `default` - Sets the default authentication method for User Logins.
- `<list-name>` - Uses the list of user names created with the user name command, for authentication.

This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Global Configuration Mode

Example

```
Your Product(config)# login authentication default
```

Related Command(s)

- `username` - Creates a user and sets the enable password for that user with the privilege level
- `no enable password` - Deletes a user and disables enable password parameters
- `show system information` - Displays system information

authorized-manager ip-source

Command Objective This command configures an IP authorized manager.

The no form of the command removes manager from authorized managers list.

Syntax

authorized-manager ip-source <ip-address> [{<subnet-mask> | / <prefix-length(1-32)>}] [interface [interface-type<0/a-b, 0/c, ...>] [interface-type <0/a-b, 0/c, ...>]] [<interface-type <a,b or a-b or a,b,c-d...>]] [vlan <a,b or a-b or a,b,c-d>] [cpu0] [service [snmp] [telnet] [http]

[https] [ssh]] no authorized-manager ip-source < ip-address > [{<subnet- mask > | / <prefix-length(1-32)>}]

Parameter Description

- `<ip-address>` - Sets the network or host address from which the switch is managed. An address 0.0.0.0 indicates 'Any Manager'."
- `<subnet-mask>` - Sets the subnet mask for the configured IP address. The configured subnet mask should be in the same subnet of the network in which the switch is placed.
- `<prefix-length(1-32)>` - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. The value ranges between 1 and 32.
- `interface` - Configures the network or host address for the specified interface. The details to be provided are:
  - `interface-type` - Sets the type of interface. The interface can be:
  - `qx-ethernet` – A version of LAN standard architecture that supports data transfer up to 40 Gigabits per second.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `interface-type <0/a-b, 0/c, ...>` - Sets the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash. Use commaas a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
- <interface-type <a,b or a-b or a,b,c-d...> - Configures the network or host address for the specified port-channel interface. Port- channel is a Logical interface that represents an aggregator which contains several ports aggregated together. Configures the port-channel interface identifier. This is a unique value that represents the specific interface. Only port-channel ID is provided port-channel. For example: 1 represents port- channel ID. Use comma as a separator without space while configuring list of interfaces. Example: 1, 2, 3 or 1-3.
- `vlan <a,b or a-b or a,b,c-d>` - Sets the list of VLANs or a single specific VLAN in which the IP authorized manager can reside.
- `cpu0` - Configures the access rights for the manager of the switch through OOB Port.
- `service` - Configures the type of service to be used by the IP authorized manager. The values can be:
- `ssh` - Logs into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure

communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist. SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force ssh to disconnect. He or she cannot play back the traffic or hijack the connection when encryption is enabled.

- `http` - Defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page
- `https` – Transmits data securely over the World Wide Web. S-HTTP is designed to transmit individual messages in a secured manner.
- `snmp` - Manages complex networks. SNMP works by sending messages, called PDUs, to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in MIBs and return this data to the SNMP requesters

Mode Global Configuration Mode

Default All services are allowed for the configured manager

Example

```
Your Product(config)# authorized-manager ip-source 10.203.113.5
255.255.255.255 interface gigabitethernet 0/1 vlan 1 service snmp
```

Related Command(s) `show authorized managers` - Displays the configured authorized managers

ip http port

Command Objective This command sets the HTTP port. This port is used to configure the router using the Web interface. The value ranges between 1 and 65535.

The no form of the command resets the HTTP port to its default value.

Syntax

ip http port <port(1-65535)>

no ip http port

Mode Global Configuration Mode

Default 80

Note: HTTP port number configuration takes effect only when HTTP is disabled and enabled again.

Example

```
Your Product(config)# ip http port 90
```

Related Command(s)

- `Set ip http` - Enables/disables HTTP

- `show http server status` - Displays the http server status

set ip http

Command Objective This command enables/disables HTTP in the switch.

Syntax **set ip http {enable | disable}**

Parameter Description

- `enable` - Enables HTTP in the switch.
- `disable` - Disables HTTP in the switch.

Mode Global Configuration Mode

Default enable

Example Your Product(config)# set ip http disable

Related Command(s)

- `ip http port` - Sets the HTTP port
- `show http server status` - Displays the http server status

mtu

Command Objective This command configures the maximum transmission unit frame size for all the frames transmitted and received on all the interfaces in a switch. The size of the MTU frame size can be increased using this command. The value ranges from 46 to 9216.

Note: This value defines the largest PDU that can be passed by the interface without any need for fragmentation. This value is shown to the higher interface sub- layer and should not include size of the encapsulation or header added by the interface. This value represents the IP MTU over the interface, if IP is operating over the interface.

Syntax **mtu <frame-size(46-9216)>**

Mode Interface Configuration Mode (Vlan / Physical/ Port channel)

Default 1500

- This configuration can be done, only if the interface is administratively down.
- The MTU value should not be greater than 1500 for fastEthernet interface.
- Any messages larger than the MTU are discarded silently by the hardware

Example `Your Product(config-if)# mtu 900`

Related Command(s)

- `show interfaces` - Displays the interface status and configuration
- `show interface mtu` - Displays the global maximum transmission unit
- `shutdown-physical/VLAN/port-channel/tunnel Interface` – Enables the physical interface/VLAN interface/port-channel interface/tunnel interface/OOB interface.

system mtu

Command Objective This command configures the maximum transmission unit frame size for all the frames transmitted and received on all the interfaces in a switch. The size of the MTU frame size can be increased using this command. The value ranges between 90 and 9216.

The no form of this command sets the maximum transmission unit to the default value in all interfaces. This value defines the largest PDU that can be passed by the interface without any need for fragmentation. This value is shown to the higher interface sub-layer and should not include size of the encapsulation or header added by the interface. This value represents the IP MTU over the interface, if IP is operating over the interface.

Note: This command is a standardized implementation of the existing command. It operates similar to that of the command mtu frame size.

Syntax **system mtu <frame-size(90-9216)>**

no system mtu

Mode Global configuration mode

Default 1500

- This configuration can be done, only if the interface is administratively down.
- Any messages larger than the MTU are discarded silently by the hardware

Example Your Product(config)# system mtu 200

Related Command(s)

- `show interfaces` - Displays the interface status and configuration
- `show interface mtu` - Displays the global maximum transmission unit

bridge port-type

Command Objective This command configures the bridge port type for an interface. It is not supported but reserved for future release.

Syntax **bridge port-type { providerNetworkPort | customerNetworkPort {port-based | s-tagged | c-tagged} | customerEdgePort | propCustomerEdgePort | propCustomerNetworkPort | propProviderNetworkPort | customerBridgePort | customerBackbonePort}**

Parameter Description

- `providerNetworkPort` - Sets the bridge port type as provider network port. This option is applicable in provider bridges and provider backbone b-component bridge modes. The port is connected to a single provider.
- `customerNetworkPort` - Sets the bridge port type as customer network port. It has the following options:
  - `port-based`– Sets the bridge port type as port based.
  - `s-tagged-`– Sets the bridge port type as s-tagged
  - `c-tagged-`– Sets the bridge port type as c-tagged
- `customerEdgePort` - Sets the bridge port type as Customer Edge Port.

  The port is in a PEB that is connected to a single customer. The packets received on this port are initially classified to a CVLAN. CVLAN classification is done based on the VID in the C-tag present in the packet or from the PVID of the port. Service instance selection is done for a frame based on the entry present in the C-VID registration table for the pair (C- VID, reception port).

- `propCustomerEdgePort` - Sets the bridge port type as Proprietary Customer Edge Port. The port is connected to a single customer, where multiple services can be provided based on only proprietary SVLAN classification tables. S-VLAN classification is not done based on C-VID registration table on the port.
- `propCustomerNetworkPort` - Sets bridge port type as Proprietary Customer Network Port. The port is connected to a single customer, where multiple service can be provided based on CVLANs by assigning one of the proprietary SVLAN classification tables to the port. The services can also be assigned using other proprietary SVLAN classification tables, where CVLAN is not the index of the table.
- `propProviderNetworkPort` - Sets bridge port type as Proprietary Provider Network Port. The port is connected to a Q-in-Q bridge located inside the provider network. The port acts as a part of S-VLAN component. The packets to be tagged and sent out of the port contain 0x8100 as its ethertype. The packets received with standard Q tags are considered as S- Tagged packets.
- `customerBridgePort` - Sets bridge port type as Customer Bridge Port.

  The port is to be used in customer bridges and in provider (Q-in-Q) bridges. This port type is not valid in PCBs and PEBs.

- `customerBackbonePort` - Sets bridge port type as Backbone Edge Bridge Port that can receive and transmit I-tagged frames for multiple customers, and assign B-VIDs and translate I-SID on the basis of the received I-SID. CBPs are applicable only on PBB B Components.

Mode Interface Configuration Mode

Default

- `providerNetworkPort` for provider core and edge bridges.

- customerBridgePort for customer bridges.
- Tunneling must be enabled to change port type from Provider Network Port.
- Tunneling must be disabled to change port type to Provider Network Port.
- Port must be administratively down for changing to another port type.
- Bridge port-type is supported only in the following Bridge Modes:
  - Provide Edge Bridge
  - Provider Core Bridge
  - Provider Backbone Bridge I Component
  - Provider Backbone Bridge B Component
- In case of Provider Bridge or Customer Bridge, bridge port type will always be customerBridgePort.
- customerEdgePort is valid only in Provider Edge Bridge.
- All other port types excluding customerBridgePort and customerEdgePort are valid in both Provide Edge Bridge and Provider Core Bridge.
- Bridge port type can be set only for switch ports and not for router ports, IVR interfaces and I- LAN interfaces.
- The port type cannot be set for a port-channel port, if physical ports are aggregated in the port-channel.
- The port type cannot be set for a port that is part of a port-channel.

Example

```
Your Product(config-if)# bridge port-type providerNetworkPort
```

Related Command(s)

- show interface bridge port-type - Displays the Bridge Port Type of interfaces in the switch
- switchport acceptable-frame-type - Configures the type of VLAN dependant BPDU frames such as GMRP BPDU, that the port should accept during the VLAN membership configuration.
- switchport ingress-filter - Enables ingress filtering feature on the port.
- tunnel mode – Configures the tunnel interface with the associated parameters.
- switchport - Configures the port as switch port.

system-specific port-id

Command Objective This command configures the system specific index for the port. It provides a different numbering space other than the IfIndex to identify ports. The value ranges between 1 and 16384. If no other value has been configured, 0 is set by default.

Syntax **system-specific port-id <integer (1-16384)>**

Mode Interface Configuration Mode

Default 0

Example

```
Your Product(config-if)# system-specific port-id 50
```

Related Command(s) `show system-specific port-id` - Displays the custom-param configurations.

set custom-param

Command Objective This command configures the custom parameters for a particular port.

The no form of the command deletes the custom parameter configurations.

Syntax **set custom-param {type <integer> length <integer> value <string> | attribute <integer (1-4)> value <integer (0-4294967295)>}**

no custom-param [type <integer>] [attribute <integer (1-4)>]

Parameter Description

- `type` - Sets the type of the TLV information.
- `length` - Sets the length of the TLV information.
- `value` - Sets the value of the TLV information.
- `attribute` - Sets the opaque attribute ID configured on the port.. The value ranges between 1 and 4.
- `value` - Sets the value for the Opaque attribute. The value ranges between 0 and 4294967295.

Mode Interface Configuration Mode

Default value - 0

Example Your Product(config-if)# set custom-param attribute 2 value 40

Related Command(s) `show custom-param` - Displays the custom-param configurations.

mac-addr

Command Objective This command configures unicast MAC address for the interface.

Syntax **mac-addr <aa:aa:aa:aa:aa:aa>**

Mode Interface Configuration Mode

Default

- MAC address of the switch is assigned as MAC address for the interface.
- The MAC address can be set only when `ifMainAdminStatus` for the interface is down.
- The object is valid only for interfaces that have the `ifMainType` set as `ethernetCsmacd(6)` or `ieee8023ad(161).`

Example

```
Your Product(config-if)# mac-addr 00:22:33:44:55:66
```

Related Command(s) `show interfaces` - Displays the interface status and configuration.

snmp trap link-status

Command Objective This command enables trap generation on the interface. The interface generated linkUp or linkDown trap. The linkUp trap denotes that the communication link is available and ready for traffic flow. The linkDown trap denotes that the communication link failed and is not ready for traffic flow. The no form of this command disables trap generation on the interface.

Syntax **snmp trap link-status**
snmp trap link-nostatus

Mode Interface Configuration Mode

Default SNMP trap link status is enabled

Example Your Product(config-if)# snmp trap link-status

Related Command(s) `show interfaces` - Displays the interface status and configuration.

Write

Command Objective This command writes the running-config to a flash file, startup-configuration file or to a remote site.

Syntax **write { flash:filename | startup-config | tftp://ip- address/filename | sftp://<user-name>:<pass-word>@ip- address/filename }**

Parameter Description

- `flash:filename` - Configures the name of the file to which the configuration is to be saved. This file is present in the flash.
- `startup-config` - Starts the switch with the saved configuration on reboot.
- `tftp` - Configures the TFTP related details for writing the configuration to a file in TFTP server.
  - `ip-address` - The IP address or host name of the server in which configuration should be maintained.
  - `filename` - The name of the file in which the configuration should be written. Filenames and directory names are case sensitive
- `sftp` - Configures the SFTP related details for writing the configuration to a file in SFTP server.
  - `user-name` - The user name of remote host or server.
  - `pass-word` – The password for the corresponding user name of remote host or server
  - `ip-address` - The IP address or host name of the server in which configuration should be maintained.
  - `filename` - The name of the file in which the configuration should be written. Filenames and directory names are case sensitive

Mode Privileged EXEC Mode

Example `Your product# write startup-config`

Related Command(s)

- `show nvram` - Displays the current information stored in the NVRAM
- `show system information` - Displays system information

copy

Command Objective This command copies the configuration from a remote site to flash.

Syntax **copy { tftp://ip-address/filename startup-config | sftp://<user-name>:<pass-word>@ip-address/filename startup- config | flash: filename startup-config | cust:/filename startup-config}**

Parameter Description

- `tftp://ip-address/filename startup-config` - Configures the address from which the file isto be copied and the file name from which configuration is to be copied. This option configures the TFTP server details Filenames and directory names are case sensitive
- `sftp://<user-name>:<pass-word>@ip-address/filename` - Configures the name of the file in remote location to be copied (downloaded) into configuration file (smis.conf). This option configures theSFTP server details. Filenames and directory names are case sensitive
- `flash: filename startup-config` - Configures the name of the file in flash. The configuration in the flash file are used. Filenames are case sensitive
- `cust:/filename startup-config` - Configures the name of the file in USB drive. The configuration in the USB flash file are used. Filenames are case sensitive.

Mode Privileged EXEC Mode

copy startup-config

Command Objective This command takes a backup of the initial configuration in flash or at a remote location.

Syntax **copy startup-config {flash: filename | tftp://ip- address/filename | sftp://<user-name>:<pass-word>@ip- address/filename | cust:/filename }**

Parameter Description

- `flash: filename` - Configures the name of the file in which the initial configuration should be stored. This file is available in the Flash.
- `tftp://ip-address/filename` - Configures the TFTP details for taking back up of initial configuration in TFTP server.
    - `ip-address` - The IP address or host name of the server.
    - `filename` - The name of the file in which the initial configuration should be stored.

Filenames and directory names are case sensitive

- `sftp://<user-name>:<pass-word>@ip-address/filename` - Configures the SFTP details for taking back up of initial configuration in SFTP server.
  - `user-name` - The user name of remote host or server
  - `pass-word` – The password for the corresponding user name of remote host or server
  - `ip-address` - The IP address or host name of the server
  - `filename` - The name of the file in which the initial configuration should be stored. Filenames and directory names are case sensitive
- `cust:/filename` - Configures the file for taking back up of-initial configuration in USB drive.

Mode Privileged EXEC Mode

Example `Your product# copy startup-config flash:clcliser`

Related Command(s)

- `copy running-config startup-config` - Copies variables from the running configuration to the startup configuration file in NVRAM
- `copy-file` - Copies a file from a source remote site /flash to a destination remote site/flash

copy running-config startup-config

Command Objective This command copies the variables from the running configuration to the startup configuration file in NVRAM, where the running-config is the current configuration in the switch and the startup config is the configuration that is loaded when the switch boots up.

Note: This command is a complete standardized implementation of the existing command. It operates similar to that of the command copy startup-config.

Syntax **copy running-config startup-config**

Mode Privileged EXEC Mode

Example `Your product# copy running-config startup-config`

Related Command(s)

- `copy startup-config` - Copies variables from the running configuration to the startup configuration file in NVRAM
- `copy-file` - Copies a file from a source remote site /flash to a destination remote site/flash

copy logs

Command Objective This command writes the system logs to a remote site.

Syntax **copy logs {tftp://ip-address/filename | sftp://<user- name>:<pass-word>@ip-**

address/filename}

Parameter Description

- tftp://ip-address/filename - Configures the TFTP details for taking back up of system logs in TFTP server.
    - `ip-address` - the IP address or host name of the TFTP server.
    - `filename` - The name of the file in which the system logs should be stored. Filenames and directory names are case sensitive
- `sftp://<user-name>:<pass-word>@ip-address/filename` - Configures the SFTP details for taking back up of system logs in SFTP server.
    - `user-name` - The user name of remote host or server.
    - `pass-word` **–** The password for the corresponding user name of remote host or server.
    - `ip-address` - The IP address or host name of the server.
    - `filename` - The name of the file in which the system logs should be stored. Filenames and directory names are case sensitive

Mode All Modes

Example

```
Your Product# copy logs tftp://10.0.0.10/clcliser
```

firmware upgrade

Command Objective This command performs firmware upgrade using TFTP from a remote location.

Syntax **firmware upgrade {tftp://ip-address/filename} {flash:normal| flash:fallback}**

Parameter Description

- `tftp://ip-address/filename` - Configures the file to be used for firmware upgrade and its source URL.
    - `ip-address` - IP address or host name of the TFTP server
    - `filename` - The name of the file to be used for firmware upgrade.

  Filenames and directory names are case sensitive

- `flash:normal` - Sets the flash in normal image.
- `flash:fallback` - Sets the fallback image in Flash

Mode Privileged EXEC Mode

In stacking environment case, this command copies the image to the attached peers.

Example

```
Your Product# firmware upgrade tftp://12.0.0.100/Ramdisk.bin flash:normal
```

Notes:

- This CLI can only work with 2.1.3-25 or later release versions for SSE-G3648B models.
- The firmware version to be used (the filename field) has to be 2.1.3-25 or later release versions.

copy - file

Command Objective This command copies a file from a source remote site /flash to a destination remote site/flash. The entire copying process takes several minutes and differs from protocol to protocol and from network to network.

Syntax **copy { tftp://ip-address/filename | sftp://<user- name>:<pass-word>@ip-address/filename | flash:filename | cust:/filename}**

{tftp://ip-address/filename | sftp://<user-name>:<pass- word>@ip-address/filename | cust:/filename | flash: filename | filename }

Parameter Description

- `tftp://ip-address/filename` - Configures the TFTP details to/from which file to be copied.
  - ip-address - IP address or host name of the TFTP server
  - filename - Name of the file to be copied or file to which information is to be copied. Filenames and directory names are case sensitive
- `sftp://<user-name>:<pass-word>@ip-address/filename` - Configures the SFTP details to / from which file to be copied.
  - `user-name` - User name of remote host or server
  - `pass-word` **–** Password for the corresponding user name of remote host or server
  - `ip-address` - IP address or host name of the server
  - `filename` - Name of the file to be copied or file to which information is to be copied. Filenames and directory names are case sensitive
- `cust:/filename` - Configures the name of the file to be copied. This file is present in USB. Filenames are case sensitive
- `flash: filename` - Configures the name of the file to be copied. This file is present in Flash. Filenames are case sensitive
- `filename` - Configures the name of the file to be copied. Filenames are case sensitive.

Mode Privileged EXEC Mode

Example Your product# copy tftp://12.0.0.2/clclirel flash:clcliser

Related Commands

- `copy running startup-config` - Copies variables from the running configuration to the startup configuration file in NVRAM
- `copy startup-config` - Copies variables from the running configuration to the startup configuration file in NVRAM

clock set

Command Objective This command manages the system clock.

Syntax **clock set hh:mm:ss <day (1-31)>{january|february|march|april|may|june|july|august|september|october|november|december} <year (2000 - 2035)>**

Parameter Description

- `hh:mm:ss` - Sets the current time. The format is hour, minutes and seconds.
    - `<day (1-31)>` - Sets the current day. It ranges between 1 and 31.
    - `january` - Sets the month as January.
    - `february` - Sets the month as February
    - `march` - Sets the month as March
    - `april` - Sets the month as April
    - `may` - Sets the month as May
    - `june` - Sets the month as June
    - `july` - Sets the month as July
    - `august` - Sets the month as August
    - `september` - Sets the month as September
    - `october` - Sets the month as October
    - `november` - Sets the month as November
    - `december` - Sets the month as December
    - `<year (2000 – 2035)>` - Sets the year. It ranges between 2000 and 2035

Mode Privileged EXEC Mode

Example

```
Your product# clock set 18:04:10 18 Oct 2015
```

Related Command(s) show clock - Displays the system clock

erase

Command Objective This command clears the contents of the startup configuration or sets parameters in NVRAM to default values.

Syntax **erase {startup-config | nvram: | flash:filename}**

Parameter Description

- `startup-config` - Clears the startup configuration file
- `nvram` - Clears the content from NVRAM
- `flash:filename` - Clears the content from the local system flash file.

Mode Privileged EXEC Mode

Example `Your Product# erase startup-config`

Related Command(s)

- `show nvram` - Displays the current information stored in the NVRAM
- `show system information`- Displays system information

cli console

Command Objective This command enables the console CLI through a serial port. The no form of the command disables console CLI.

Syntax **cli console**

no cli console

Mode Privileged EXEC Mode

Default Enabled

This command takes effect only on system restart.

Example Your Product# cli console

Related Command(s) `show nvram` - Displays the current information stored in the NVRAM.

flowcontrol

Command Objective This command is used to set the send or receive flow-control value for an interface.

- If flowcontrol send is on for a device and if it detects any congestion at its end, then it notifies the link partner or the remote device of the congestion by sending a pause frame.
- If flowcontrol receive is on for the remote device and it receives a pause frame, then it stops sending any data packets. This prevents any loss of data packets during the congestion period.
- PAUSE is a flow control mechanism that is implied on full duplex Ethernet link segments. The mechanism uses MAC control frames to carry the PAUSE commands.

Interface must first be made administratively down before setting flow control status

Syntax **flowcontrol { send | receive} { on | off | desired}**

Parameter Description

- `send` - Sets the interface to send flow control packets to a remote device
- `receive` - Sets the interface to receive flow control packets from a remote device

- `on` - If used with receive allows an interface to operate with the attached device to send flow control packets. If used with send the interface sends flowcontrol packets to a remote device if the device supports it
- `off` - Turns-off the attached devices (when used with receive) or the local ports (when used with send) ability to send flow-control packets to an interface or to a remote device respectively
- `desired` - Allows a local port to operate with an attached device that is required to send flow control packets or that may send the control packets, when used with receive option. Allows the local port to send administrative status to a remote device if the remote device supports it, when used with send option.

Mode Interface Configuration Mode

Default The default flow control for the interfaces are:

- `flowcontrol receive off`
- `flowcontrol send off`

Example

```
Your Product(config-if)# flowcontrol send on
```

Related Command(s)

- `show interfaces` - Displays the interface status and configuration
- `show flow-control` - Displays the flowcontrol information

tunnel mode

Command Objective This command configures the tunnel interface with the associated parameters. This tunnel feature is not supported.

The no form of the command deletes the tunnel interface and its associated parameters.

Syntax **tunnel mode {gre|sixToFour|isatap|compat|ipv6ip} [config-id <ConfId(1-2147483647)>] source <TnlSrcIP/IfName> [dest <TnlDestIP>]**

no tunnel mode {gre|sixToFour|isatap|compat|ipv6ip} [config-id <ConfId(1-2147483647)>] source <TnlSrcIP/IfName/IfIndex> [dest <TnlDestIP>]

Parameter Description

- `gre` - Sets the tunnel in Generic Router Encapsulation mode.
- `sixToFour` - Sets the tunnel in six to four encapsulation mode.
- `isatap` - Sets the tunnel in ISATAP Encapsulation mode.
- `compat` - Sets the tunnel in IPv6 auto compatible encapsulation mode.
- `ipv6ip` - Sets the tunnel in IPv6 over IPv6 configured encapsulation mode.
- `config-id<ConfId(1-2147483647)>` - Sets an identifier to distinguish between multiple tunnels of the same encapsulation method, with same end-points. This value ranges between 1 and 2147483647.

- `source<TnlSrcIP/IfName>` - Sets the local end point address of the tunnel
- `dest<TnlDestIP>` - Sets the remote end point address of the tunnel

Mode Interface Configuration Mode (Tunnel interface mode)

Example `Your Product(config-if)# tunnel mode ipv6ip`

Related Command(s) `show interfaces` - Displays the interface status and configuration

tunnel checksum

Command Objective This command enables end-to-end check summing of packets. This feature is not supported.

The no form of the command disables end-to-end check summing of packets.

Syntax **tunnel checksum**
no tunnel checksum

Mode Interface Configuration Mode (Tunnel Interface mode)

Default Disabled

This command is applicable only for GRE Encapsulation Method.

Example `Your Product(config-if)# tunnel checksum`

Related Command(s) `show interfaces` - Displays the interface status and configuration

tunnel path-mtu-discovery

Command Objective This command enables Path MTU discovery on Tunnel. It is not supported.

The no form of the command disables Path MTU discovery on Tunnel.

Syntax **tunnel path-mtu-discovery [age-timer {<integer (5-254)> |infinite}]**
no tunnel path-mtu-discovery

Parameter Description

- `<integer (5-254)>` - Configures timeout in minutes, after which the estimate of the PMTU is considered stale. This value ranges between 5 and 254.
- `infinite` - Configures the PMTU timeout as infinite. Does not detect any increase in PMTU.

Mode Interface Configuration Mode (Tunnel Interface mode)

Default Disabled

Example Your Product(config-if)# tunnel path-mtu-discovery age- timer 5

Related Command(s) `show interfaces` - Displays the interface status and configuration

tunnel udlr

Command Objective This command associates tunnel with a unidirectional interface. It is not supported.

The no form of the command associates tunnel with a Bidirectional interface.

Syntax **tunnel udlr {receive-only | send-only}**

no tunnel udlr

Parameter Description

- `receive-only` - Sets the uni-directional tunnel as incoming only.
- `send-only` - Sets the uni-directional tunnel as outgoing only.

Mode Interface Configuration Mode (Tunnel interface mode)

Example

```
Your Product(config-if)# tunnel udlr receive-only
```

Related Command(s) `show interfaces` - Displays the interface status and configuration

Shutdown - physical/VLAN/port-channel/tunnel Interface

Command Objective This command disables a physical interface / VLAN interface / port-channel interface / tunnel interface.

The no form of the command enables a physical interface /VLAN interface/port-channel interface/tunnel interface.

Syntax **Shutdown**

no shutdown

Mode Interface Configuration Mode for physical interface/port-channel/tunnel interface/OOB Interface/VLAN Interface Mode for VLAN interface

Default

- The Management Interface is always enabled
- The interface VLAN 1 is enabled
- The other interfaces are disabled

Note: All functions on the specified interface are disabled by the shutdown command

Example `Your Product(config-if)# shutdown`

Related Command(s)

- `show spanning-tree` - Summary, Blockedports, Pathcost, redundancy - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree` – layer 2 gateway port - Displays spanning tree information for all L2GPs enabled in the switch.
- `show spanning-tree mst` - CIST or specified mst Instance - Displays multiple spanning tree information for all MSTIs in the switch.
- `show interfaces` - Displays the interface status and configuration

debug interface

Command Objective This command sets the debug traces for all the interfaces.

The no form of the command resets the configured debug traces.

Syntax **debug interface [track] [enetpktdump] [ippktdump] [arppktdump] [trcerror] [os] [failall] [buffer] [all]**

no debug interface [track] [enetpktdump] [ippktdump] [arppktdump] [trcerror] [os] [failall] [buffer] [all]

Parameter Description

- `track` - Generates debug messages for all track messages.
- `enetpktdump` - Generates debug messages for ethernet packet dump messages.
- `ippktdump` - Generates debug messages for IP protocol related packet dump messages.
- `arppktdump` - Generates debug messages for address resolution protocol related packet dump messages.
- `trcerror` - Generates debug messages for trace error messages.
- `os` - Generates debug messages for for OS resources. For example, when there is a failure in mem pool creation / deletion, this trace level is used
- `failall` - Generates debug messages for all failures including packet validation.
- `buffer` - Generates debug messages for buffer trace levels where packet buffer is used.i.e in cases wher packet is enqueued
- `all` - Generates debug messages for all kinds of traces.

Mode Privilege EXEC mode

Example `Your product# debug interface track`

debug-logging

Command Objective This command configures the logging option of debug traces. Debug logs are directed to the console screen or to the buffer or to a file, which can later be uploaded, based on the input.

The no form of the command displays debug logs in the console..

Syntax **debug-logging { console | file | flash}**
no debug-logging

Parameter Description

- `console` - Specifies the logging of traces at the console
- `file` - Specifies the logging of traces to a system buffer memory
- `flash` - specifies the logging of traces into a file

Mode Global Configuration Mode
Default console

Example `Your Product(config)# debug-logging console`

Related Command(s) `show debug-logging` - Displays the debug logs stored in file

incremental-save

Command Objective This command enables/disables the incremental save feature.

Syntax **incremental-save { enable | disable }**

Parameter Description

- `enable` - Enables the incremental save feature.
- `disable` - Disables the incremental save feature.

Mode Global Configuration Mode

Default enable

Example Your Product(config)# incremental-save enable

Related Command(s) `show nvram` - Displays the current information stored in the NVRAM.

auto-save trigger

Command Objective This command enables/disables the auto save trigger function.

Syntax **auto-save trigger { enable | disable }**

Parameter Description

- `enable` - Enables the auto save trigger function.
- `disable` - Disables the auto save trigger function.

Mode Global Configuration Mode

Default disable

Related Command(s) `show nvram` - Displays the current information stored in the NVRAM.

set switch maximum - threshold

Command Objective This command sets the switch maximum threshold values of RAM, CPU, and Flash. When the current resource usage rises above the threshold limit, the SNMP trap message with maximum severity will be sent for the specified resource and the syslog message will be displayed. This threshold value is represented in percentage and ranges between 1 and 100 percentage

Syntax **set switch maximum { RAM | CPU | flash } threshold<percentage (1-100)>**

Parameter Description

- `RAM` - Indicates the maximum RAM usage of the switch in percentage. When the RAM usage crosses the threshold percentage, an SNMP trap with maximum severity will be sent to the manager.
- `CPU` - Indicates the maximum CPU usage of the switch in percentage. When CPU load exceeds the threshold value, an SNMP trap with maximum severity will be sent to the manager.
- `flash` - Indicates the maximum flash usage of the switch in percentage. When the flash usage crosses the threshold percentage an SNMP trap with maximum severity will be sent to the manager.
- `percentage (1-100)` - Configures the threshold value in percentage . This value ranges between 1 and 100 percentage

Mode Global Configuration Mode

Default

- RAM - 100%
- CPU - 100 %
- flash - 100%

Example

```
Your Product(config)# set switch maximum RAM threshold 98
```

Related Command(s) `show env` – Displays the switch related information such as CPU, Flash and RAM usage, and also displays the current power and temperature of the switch

set switch temperature - threshold

Command Objective This command sets the maximum and minimum temperature threshold values of the switch in Celsius. When the current temperature drops below the threshold, an SNMP trap with maximum severity will be sent to the manager. This threshold value ranges between -14 and 40 degree Celsius.

Note: This command is a complete standardized implementation of the existing command set switch maximum - threshold.

Syntax **set switch temperature {min|max} threshold <celsius (-14- 40)>}**

Parameter Description

- `min` - Sets the minimum temperature threshold value for the switch. When the current temperature drops below the threshold, an SNMP trap with maximum severity will be sent to the manager
- `max` - Sets the maximum temperature threshold value for the switch. When the current temperature rises above the threshold, an SNMP trap with maximum severity will be sent to the manager

Mode Global Configuration Mode

Default

- min - 10 degree Celsius
- max - 40 degree Celsius

Example

```
•   Your Product(config)# set switch temperature min threshold -10
•   Your Product(config)# set switch temperature max threshold 37
```

Related Command(s) `show env`- Displays the switch related information such as CPU, Flash and RAM usage, and also displays the current power and temperature of the switch

set switch power - threshold

Command Objective This command sets the maximum and minimum threshold values of the switch power supply in volts. When the current temperature drops below the threshold, an SNMP trap with maximum severity will be sent to the manager. This threshold value ranges between 100 and 230Volts.

Note: This command is a complete standardized implementation of the existing command set switch temperature - threshold

Syntax **set switch power {min|max} threshold <volts (100-230)>**

Parameter Description

- `min` - Sets the minimum threshold power supply for the switch. When the voltage drops below the threshold, an SNMP trap with maximum severity will be sent to the manager
- `max` - Sets the maximum threshold power supply for the switch. When the voltage rises above the threshold, an SNMP trap with maximum severity will be sent to the manager

Mode Global Configuration Mode

Default

- min - 100 Volts
- max - 230 Volts

Example

```
•  Your Product(config)# set switch power min threshold 110
•  Your Product(config)# set switch power max threshold 220
```

Related Command(s) `show env`- Displays the switch related information such as CPU, Flash and RAM usage, and also displays the current power and temperature of the switch

mac-learn-rate

Command Objective This command configures the maximum number of unicast dynamic MAC (L2) MAC entries hardware can learn on the system, in a configured time interval. In next subsequent time interval, hardware can learn number of previously learnt MAC entries plus present MAC entries, this cycle will continue until MAC learning reaches to maximum number of L2 unicast dynamic entries learning capacity of the system. If rate limit is changed while timer is running, new rate limit value takes effect on next timer restart. This limit is to control the number of MAC entries indication to control plane from hardware, when hardware MAC learning is enabled. Configuration value '0' disables this feature in the system.

The no form of the command removes the limit on number of unicast MAC entry indications (limit value is set as 0) and resets the configured time interval to default value.

Note: This command is not supported in MBM-XEM-002.

Unsupported Commands

Syntax **mac-learn-rate {<no of MAC entries(0-2147483647)>} [interval {<milliseconds(1-100000)>}]no mac-learn-rate**

Parameter Description

- `<no of MAC entries(0-2147483647)>` - Configures the maximum number of unicast dynamic MAC (L2) entries that can be learned in the switch within the specified time interval. The configured value takes effect on next timer restart, if this value is changed while the timer is running. This value is used to control the number of MAC entries indicated to control plane from the hardware, when hardware MAC learning is enabled. The value ranges between 0 and 2147483647. The value 0 represents that no limit is set in the switch. This limit value does not impose any restrictions on multicast / broadcast and dynamic / static / protocol (MMRP) MAC learning capability limits.

- `interval<milliseconds(1-100000)>` - Configures the time interval (in milliseconds) for maximum number of MAC entries to be learned in the switch. The configured value takes effect from the next timer restart. The value ranges between 1 and 100000 milliseconds.

Mode Global Configuration mode

Default

- `<no of MAC entries(0-2147483647)>` - 1000
- `interval` – 1000

Example `Your Product(config)# mac-learn-rate 100 interval 50`

Related Command(s) `show mac-learn-rate` - Displays the maximum limit on number of MAC learning indications to control plane from hardware and the MAC learning limit rate interval.

system contact

Command Objective This command sets the system contact information.

Syntax **system contact <contact info>**

Mode Global Configuration Mode

Example Your Product(config)# system contact support@x.com

Related Command(s) `show system information` - Displays system information.

system location

Command Objective This command sets the system location.

Syntax **system location <location name>**

Mode Global Configuration Mode

Example Your Product(config)# system location Controls

Related Command(s) `Show system information` - Displays system information.

clear interfaces - counters

Command Objective This command clears all the current interface counters from the interface unless the optional arguments type and number are specified to clear only a specific interface type (serial, Ethernet, Token Ring, and so on).

Syntax **clear interfaces [<interface-type> <interface-id>]counters**

Parameter Description

- `<interface-type>` - Displays the IP interface configuration for the specified type of interface. The interface can be:
    - `qx-ethernet` **–** A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` **–** A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
    - `extreme-ethernet` **–** A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `internal-lan` **–** Internal LAN created on a bridge per IEEE 802.1ap.
- `<interface-id>` - Displays the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1represents that the slot number is 0 and port number is 1.

Mode Privileged EXEC Mode

Example `Your product# clear interfaces counters`

Related Command(s)

- `show interfaces - counters` - Displays the interface statistics for each port.
- `show interfaces` - Displays the interface status and configuration

clear counters

Command Objective This command clears all the current interface counters from the interface unless the optional arguments type and number are specified to clear only a specific interface type (serial, Ethernet, Token Ring, and so on).

Note: This command is a standardized implementation of the existing command and operates similar to that of the command clear interfaces - counters.

Syntax **clear counters [<interface-type> <interface-id>]**

Parameter Description

- `<interface-type>` - Displays the IP interface configuration for the specified type of interface. The interface can be:
    - `qx-ethernet` **–** A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` **–** A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

  - o `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Displays the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1represents that the slot number is 0 and port number is 1.

Mode Privileged EXEC Mode

Example `Your product# clear counters`

Related Command(s)

- `show interfaces counters` - Displays the interface statistics for each port.
- `show interfaces` - Displays the interface status and configuration

show ip interface

Command Objective This command displays the IP interface configuration.

Syntax **show ip interface loopback <loopback-id(0-100)>]**

show ip interface [vrf <vrf-name>] [{[Vlan <vlan-id(1-4094)> [switch <switch-name>]] | [<interface-type> <interface-id>] | [loopback <loopback-id(0-100)>]}]

Parameter Description

- `vrf<vrf-name>` - Displays IP interface for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32
- `Vlan<vlan-id(1-4094)>` - Displays the IP interface configuration for the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
- `switch<switch-name>` - Configures IP interface for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. This feature has been included to adhere to the Industry Standard CLI syntax.
- `<interface-type>` - Displays the IP interface configuration for the specified type of interface. The interface can be:
  - o `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - o `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - o `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Displays the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number

and port number separated by a slash. For example: 0/1represents that the slot number is 0 and port number is 1.

- `loopback<loopback-id(0-100)>` - Displays the IP interface configuration for the specified loopback ID. This is a unique value that represents the specific loopback created. The value ranges between 0 and 100.

Mode Privileged EXEC Mode

Default vrf - default

Note: If executed without the optional parameters this command displays the IP interface statistics and configuration for all the available interfaces.

Example

```
Your product# sh ip interface vrf default
vlan1 is up, line protocol is up
Internet Address is 12.0.0.1/8
Broadcast Address 12.255.255.255 vlan2 is up, line protocol is up Internet
Address is 15.0.0.1/8
Broadcast Address 15.255.255.255
```

Related Command(s)

- `ip address` - Sets the IP address for an interface
- `switchport` - Configures the port as switch port
- `release` - Releases, on the specified interface, the DHCP lease obtained for an IP address from a DHCP server.
- `renew` - Renews the DHCP lease for the interface specified.
- `show interfaces` - Displays the interface status and configuration

show authorized-managers

Command Objective This command displays the configured authorized managers' related information available in the switch.

Syntax **show authorized-managers [ip-source < ip-address >]**

Parameter Description `ip-source< ip-address >`- Displays the configured authorized manager related information for the specified network or host address.

Mode Privileged EXEC Mode

Example

```
Your product# show authorized-managers
Ip Authorized Manager Table
-------------------------------------------
Ip Address    : 12.0.0.1
Ip Mask       : 255.255.255.255
Services allowed     : ALL Ports allowed    : Gi0/1
On cpu0       : Deny
Vlans allowed        : All Available Vlans
```

Related Command(s) `authorized-manager ip-source` - Configures an IP authorized manager

show interfaces

Command Objective This command displays the interface status and configuration.

Syntax **show interfaces [{ [<interface-type> <interface-id>] [{ description | storm-control | flowcontrol | capabilities | status | port-security-state }] | {vlan <vlan-id/vfi-id>[{switch <switch-name>}]} | tunnel <tunnel-id (0-128)> | private-vlan mapping}]**

Parameter Description

- `<interface-type>` - Displays the interface status and configuration for the specified type of interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Displays the interface status and configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1. description - Displays the admin status and protocol status for the specified interface.
- `Description` - Displays the interface description.
- `storm-control` - Displays the broadcast, multicast, and unicast storm control suppression levels for the specified interface
- `flowcontrol` - Displays the flow control related statistics information for the specified interface.
- `capabilities` - Displays the interface type, interface speed, duplex operation and flowcontrol status for the specified interface.
- `status` - Displays the status, duplex details, speed and negotiation mode of the specified interface.
- `port-security-state` - Displays the state of the port security option.
- `vlan <vlan-id/vfi-id>`- Displays the interface status and configuration for the specified VLAN/ VFI ID. This value ranges between 1 and 65535.
  - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - `<vfi-id>`. - VFI ID is a VLAN created in the system which contains Pseudo wires and

Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535.

Notes:

1. This interface type is not supported. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- `switch<switch-name>` - Configures IP interface for the specified context.

  Note: This value represents unique name of the switch context. This value is a string whose maximum size is 32 This parameter is specific to multiple instance feature. This feature has been included to adhere to the Industry Standard CLI syntax
- `tunnel<tunnel-id (0-128)>` - Displays the interface status and configuration for the specified tunnel ID. This is a unique value that represents the specific tunnel created. The value ranges between 0 and 128.
- `private-vlan mapping` - Displays list of secondary VLAN to the primary VLAN IVR interface, so that both VLANs share the same primary VLAN.

Mode Privileged EXEC Mode

Example

```
Your product# show interfaces gigabitethernet 0/1
Gi0/1 up, line protocol is up (connected) Bridge Port Type: Customer Bridge Port Hardware
Address is 00:01:02:03:04:22
RARP Client is enabled
MTU  1500 bytes, Full duplex, 100 Mbps,  Auto-Negotiation
HOL Block Prevention enabled. Invalid flowcontrol Mode
Link Up/Down Trap is enabled
Reception Counters
Octets                     : 0
Unicast Packets            : 0
Discarded Packets          : 0
Error Packets              : 0
Unknown Protocol           : 0
Transmission Counters
Octets                     : 8266
Unicast Packets            : 0
Discarded Packets          : 0
Error Packets              : 0
Your product# show interfaces description
Interface                Status         ProtocolDescription
```

```
Gi0/1-                       -up-          -up-
Gi0/2                        up            up
vlan1                        up            up
ac1                          down          down
Your product# show interfaces gigabitethernet 0/2 storm control
Gi0/2                                                        -
DLF Storm Control                   : Disabled
DLF Storm Control Limit      : 0
Broadcast Storm Control      Enabled
Broadcast Storm Control      : 0
Multicast Storm Control      Enabled
Multicast Storm Control      : 0
Your product# show interfaces gigabitethernet 0/2 flow- control
Port Tx  FlowControl Rx Flow Control Tx Pause  Rx      Pause HC      TxPause  HC R
-------- -----------    -------- ------        -----  --------      ----------
Gi0/2    off            off      0             0      0             0
Your product# show interfaces gigabitethernet 0/2 capabilities
Gi0/2
Type                         : 10/100/1000 Base TX
Speed                        : 10, 100, 1000, Auto
Duplex                       : Half, Full
FlowControl                : Send, Receive
Your product# show interfaces gigabitethernet 0/2 status
Port                         Status        Duplex        Speed         Negotiation
-------                      ----------    ----------    ----------    --------------------
Gi0/2                        connected     Full          100 Mbps      Auto
Your product# show interfaces vlan 1
vlan1 up, line protocol is up (connected)
Your product# show interfaces port-channel 2
po2 up, line protocol is up (connected)
Your product# show interfaces tunnel 0 tunnel0 up, line protocol is up (connected)
Hardware is Tunnel
MTU 1480 bytes
Encapsulation TUNNEL
Tunnel Source 12.0.0.2,Destination 12.0.0.3
Tunnel Protocol/transport IPV6IP Checksumming of
packets Disabled Path MTU Discovery Disabled
```

Related Command(s)

- `interface` - Enters the interface mode and allows the user to execute all the commands that supports interface configuration mode.
- `Interface-configuration and deletion` - Configures interface such as out of band management, port channel, tunnel and so on
- `Snmp trap link-status` - Enables trap generation on the interface.
- `Storm-control` - Sets storm control rate for broadcast, multicast and DLF packets
- `flowcontrol` - Enables flow-control
- `show flow-control` - Displays the flow-control information
- `mac-addr` - Configures MAC address for the interface.
- `tunnelmode` - Configures the tunnel interface with the associated parameters.
- `tunnel checksum` - Enables end-to-end checksumming of packets.
- `tunnel path-mtu-discovery` - Enables Path MTU discovery on Tunnel.

- `tunnel udlr` - Associates tunnel with a unidirectional interface.
- `shutdown` – physical/VLAN/port-channel/tunnel interface Disables a physical interface / VLAN interface / port-channel interface / tunnel interface.

show interfaces - counters

Command Objectives This command displays the interface statistics for each port.

Syntax **show interfaces {counters | HC counters} [{ <interface- type> <interface-id> | vlan <vlan_vfi_id> [switch <switch- name>] | tunnel <tunnel-id(0-128)> | ppp <ppp-id(1-4094)>}]**

Parameter Description

- `counters` - Displays the interface statistics for all the available interfaces.
- `HC counters` -.Displays the interface incoming and outgoing traffic statistics for the for the HC port.
- `<interface-type>` - Displays the interface incoming and outgoing traffic statistics for the specified type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplexlinks.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Displays the counters for the interface incoming and outgoing traffic statistics for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. For interface type port-channel, for example: 1 represents port-channel ID.
- `vlan <vlan_vfi_id>` - Displays the interface statistics for the specified VLAN/ VFI ID. This value ranges between 1 and 65535.
    - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
    - `<vfi-id>.` - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535, this interface type is not supported.

Notes:

        1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
        2. VFI IDs 4096 and 4097 are reserved id entifiers used in MPLS PW.
        3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
    - `switch<switch-name>` - Displays interface statistics for the specified context. This value represents unique name of the switch context. This value is a string with the maximum length as 32 This parameter is specific to multiple instance feature. This feature has been included to adhere to the Industry Standard CLI syntax
- `tunnel<tunnel-id(0-128)>` - Displays the counters for the interface incoming and outgoing traffic statistics for the tunnel identifier. This is a unique value that represents the specific tunnel created. The value ranges between 0 and 128.
- ppp<short(1-4094)> - Displays the counters for the interfaces of the point to point protocol. This value ranges between 1 and 4094.

Mode Privileged EXEC Mode

Example `Your Product# show interfaces counters`

```
Port              InOctet  InUcast      InDiscard    InErrs        InHCOctet
Gi0/1             115043   1380         690          0             115043
vlan1             0        0            0            0             0
vlan10            0        0            0            0             0
Port              OutOctet OutUcast     OutDiscard   OutErrs       OutHCOctet
Gi0/1             12145    0            0            0             12145
vlan1             120      1            0            0             120
vlan10            0        0            0            0             0
Your Product# show interfaces counters vlan 10
Port              InOctet  InUcast      InDiscard    InErrs        InHCOctet
----              -------  -------      ---------    ------        ---------
vlan10            0        0            0            0             0
Port              OutOctet OutUcast     OutDiscard   OutErrs       OutHCOctet
----              -------- --------     ----------   -------       ---------
vlan10            0        0            0            0             0
Your Product # show interfaces HC counters
Port              InHCOctet      InUcastPkts         InMulticastPkts
----              ---------      -----------         ---------------
Gi0/1             129886         0                   0
vlan1             0              0                   0
vlan10            0              0                   0
Port                OutHCOctet   OutUcastPkts        OutMulticastPkts
-------------------------------                      ----------------
Gi0/1             14071          0                   0
vlan1             120            0                   0
vlan10            0              0                   0
Your Product# show interfaces HC counters gi 0/1
Port              InHCOctet      InUcastPkts         InMulticastPkts
```

```
----              ----------      -----------      --------------
Gi0/1             153868          0                0
Port              OutHCOctet      OutUcastPkts     OutMulticastPkts
------------------------------------------------   ----------------------------
Gi0/1             16730           0                0
```

Related Command(s) `interface` - configure interface such as out of band management, port channel, tunnel and so on

show system-specific port-id

Command Objective This command displays the system specific index configuration for all interfaces for which this configuration is done.

Syntax **show system-specific port-id**

Mode Privileged EXEC Mode

Example

```
Your product# show system-specific port-id
Interface PortID
Slot0/1   45
```

Related Command(s) `system-specific port-id` - Configures the system specific index for the port.

show custom-param

Command Objective This command displays the custom-param configurations done in the switch.

Syntax **show custom-param**

Mode Privileged EXEC Mode

Example

```
Your product# show custom-param
Slot0/1
AttrID        AttrValue
------------  --------------
4             5454
Slot0/2
AttrID        AttrValue
------------  --------------
2             2424
Type        Length    Value
------------ ------------ ------------
2           4         root
5           4         root
```

Related Command(s) `Set custom-param` - Configures the custom-param for a particular port.

show interface mtu

Command Objective This command shows the Maximum Transmission Unit (MTU) of ports in the switch.

Syntax **show interface mtu [{Vlan <vlan-id/vfi-id> [switch <switch-name>] | port-channel <port-channel-id (1-65535)> | <interface-type> <interface-id> }]**

Parameter Description

- `Vlan <vlan-id/vfi-id>` - Displays the MTU value for the specified VLAN/ VFI ID. This value ranges between 1 and 65535.
    - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
    - `<vfi-id>.` - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096and 65535. This interface type is not supported.

      Notes:

      - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
      - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
      - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- `switch <switch-name>` - Configures IP interface for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. This feature has been included to adhere to the Industry Standard CLI syntax
- `port-channel<port-channel-id (1-65535)>` - Displays the MTU value for the specified port-channel ID. This is a unique value that represents the specific port-channel created. This value ranges between 1 and 65535.
- `<interface-type>` - Displays the MTU value for the specified type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.

- `<interface-id>` - Displays the MTU value for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.

Mode Privileged EXEC Mode

Example

```
Your product# show interface mtu Vlan 1
vlan1   MTU size is 1500
```

Related Command(s) `mtu`- Configures the maximum transmission unit frame size for the interface

show interface bridge port-type

Command Objective This command displays the bridge port type of all interfaces available in the switch.

Syntax **show interface bridge port-type [{ port-channel <integer(1-65535)> | <interface-type> <ifnum> | pw <integer (1-65535)> }]**

Parameter Description

- port-channel <integer (1-65535)> - Displays the bridge port type for the specified port-channel ID. This is a unique value that represents the specific port-channel created. This value ranges between 1 and 65535.
- <interface-type> - Displays the bridge port type for the specified type of interface. The interface can be:
  - qx-ethernet **–** A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet **–** A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - extreme-ethernet **–** A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
- <ifnum> - Displays the bridge port type for the specified interface identifier.

  Note: This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.

- pw <integer (1-65535)> - Displays the bridge port type for the specified pseudo wire interface. This value ranges between 1 and 65535. Maximum number of PseudoWire interfaces supported in the system is 100. This interface type is not supported.

Mode Privileged EXEC Mode

Example

```
Your product# show interface bridge port-type Gi0/1 Bridge port type is
Customer Bridge Port Gi0/2 Bridge port type is Customer Bridge Port
Gi0/3 Bridge port type is Customer Bridge Port Gi0/4 Bridge port type is
Customer Bridge Port Gi0/5 Bridge port type is Customer Bridge Port Gi0/6
Bridge port type is Customer Bridge Port Gi0/7 Bridge port type is Customer
Bridge Port Gi0/8 Bridge port type is Customer Bridge Port
Gi0/9 Bridge port type is Customer Bridge Port Gi0/10 Bridge port type is
Customer Bridge Port Gi0/11 Bridge port type is Customer Bridge Port Gi0/12
Bridge port type is Customer Bridge Port Gi0/13 Bridge port type is
Customer Bridge Port Gi0/14 Bridge port type is Customer Bridge Port Gi0/15
Bridge port type is Customer Bridge Port Gi0/16 Bridge port type is
Customer Bridge Port Gi0/17 Bridge port type is Customer Bridge Port Gi0/18
Bridge port type is Customer Bridge Port Gi0/19 Bridge port type is
Customer Bridge Port Gi0/20 Bridge port type is Customer Bridge Port Gi0/21
Bridge port type is Customer Bridge Port Gi0/22 Bridge port type is
Customer Bridge Port Gi0/23 Bridge port type is Customer Bridge Port Gi0/24
Bridge port type is Customer Bridge Port
```

Related Command(s) `bridge port-type` - Configures the bridge port type

show nvram

Command Objective This command displays the current information stored in the NVRAM.

Syntax **show nvram**

Mode Privileged EXEC Mode

Example

```
Your product# show nvram
Default IP Address                             : 12.0.0.5
Default Subnet Mask                            : 255.0.0.0
Default IP Address Config Mode                 : Manual
Default IP Address Allocation Protocol         : DHCP
Switch Base MAC Address                        : 00:25:90:03:04:01
Default Interface Name                         : 0
Default RM Interface Name                      : lo:5
Config Restore Option                          : No restore
Config Save Option                             : No save
Auto Save                                      : Disable
Incremental Save                               : Disable
Roll Back                                      : Enable
Config Save IP Address                         : 192.168.100.102
Config Save Filename                           : smis.conf
Config Restore Filename                        : smis.conf
PIM Mode                                       : Sparse Mode
IGS Forwarding Mode                            : MAC based
Cli Serial Console                             : Yes
SNMP EngineID                                  80.00.08.1c.04.46.53
SNMP Engine Boots                                    : 55
Default VLAN Identifier                              : 1
Stack PortCount                                      : 0
ColdStandby                                          : Disable
Store Default Value                                  : Disable
Vrf Unique Mac                                       : Disable
Hitless Restart Flag                                 : Disable
Hardware Version                                     : 1.0.2
Firmware Version                                     : 2.0.0
Hardware Part Number                                 : MBM-XEM-002
Software Serial Number                               : 1-0-0
Software Version                                     : 6.12.0
Switch Name                                          : SMIS
RM Heart Beat Mode                                   : Internal
RM Redundancy Type                                   : Hot
RM Data Plane Type                                   : Shared
RM Type                                              : OOB
NPAPI mode                                           : Synchronous
TimeStamp Method                                     : Software
Restore Flag                                         : Disabled
Dynamic Port Count                                   : 64
FIPS operation mode                                  : Disabled
Restore Option                                       : Disabled
Bridge Mode                                          : Customer Bridge
Management Port                                      : Disabled
Automatic Port Create Flag                           : Enabled
```

Related Command(s)

- `default mode` - Configures the mode by which the default interface acquires its IP address
- `default restore-`file - Configures the default restoration file
- `ip address` - Sets the IP address for an interface
- `login authentication` - Sets the authentication method for user logins
- `write` - Writes the running-config to a file in flash, startup-configuration file or to a remote site
- `erase`- Clears the contents of the startup configuration or sets parameters in NVRAM to default values
- `default ip address allocation protocol` - Configures the protocol by which the default interface acquires its IP address
- `incremental-save` - Enables/disables the incremental save feature.
- `auto-save trigger` - Enables/disables the auto save trigger function.
- `cli console` - Enables the console CLI through a serial port
- `automatic-port-create` - Enables or disables the Automatic Port Create feature.

show env

Command Objective This command displays the status of the all the resources like CPU, Flash and RAM usage, and also displays the current, power and temperature of the switch.

Note: This command is a complete standardized implementation of the existing command.

Note: This command is not supported in all models.

Syntax **show env {all | temperature | fan | RAM | CPU | flash |power}**

Parameter Description

- **all** - Displays threshold information of all resources such as CPU, Flash, RAM, power and temperature.
- **temperature** - Displays temperature threshold values of the switch in celciu
- **fan** - Displays the threshold information of the fan
- **RAM** - Displays the maximum RAM usage of the switch in percentage.
- **CPU** - Displays the maximum CPU usage of the switch in percentage.
- **flash** - Displays the maximum flash usage of the switch in percentage.
- **power** - Displays the threshold power suply for the switch

Mode Privileged EXEC Mode

Example

```
Your product# show env all
RAM Threshold                           : 98%
Current RAM Threshold                   : 97%
CPU Threshold                           : 92%
Current CPU Threshold                   : 0%
Fan Status 1                            : Operational
Min power supply                        : 110v
Max power supply                        : 220v
Current power supply                    : 230v
Max Temperature                         : 37C
Min Temperature                         : -10C
Current Temperature                     : 40C
Flash Threshold                         : 90%
Current Flash Threshold                 : 62%
Mgmt Port Routing                       : Disabled
Your product# show env RAM
RAM Threshold                           : 98%
Current RAM Threshold                   : 97%
Your product# show env power
Min power supply                        : 110v
Max power supply                        : 220v
Current power supply                    : 230v
```

Related Command(s)

- `set switch maximum` - threshold - Sets the switch maximum threshold values of RAM, CPU, and Flash.
- `set switch temperature` - threshold - Sets the maximum and minimum temperature threshold values of the switch.
- `set switch power` - threshold - Sets the maximum and minimum threshold values of the switch power supply.

show system information

Command Objective This command displays system information.

Syntax **show system information**

Mode Privileged EXEC Mode

Example

```
Your product# show system information
Hardware Version                        : 1.0.1
Firmware Version                        : 2.0.0
Hardware Part Number                           : MBM-XEM-002
Software Serial Number                  : 1-0-0
Software Version                        : 2.0.0
Switch Name                             : SMIS
System Contact                          : Supermicro
System Location                         : Supermicro
Logging Option                          : Console
Logging Login Authentication Mode       : Local
Config Save Status                      : Not Initiated
Remote Save Status                      : Not Initiated
Config Restore Status                   : Not Initiated
Traffic Separation Control              : none
```

Related Command(s)

- `login authentication` - Sets the authentication method for user logins
- `system contact` - Sets the system contact information
- `system location` - Sets the system location
- `debug-logging` - Configures the displays of debug logs.
- `config-restore` - Configures the startup configuration restore option.
- `set switch-name` - Sets the name of the switch.
- `Traffic seperation control` - Configures the method for receiving control packets to CPU.

show flow-control

Command Objective This command displays the flow-control information.

Syntax **show flow-control [interface <interface-type> <interface- id>]**

Parameter Description

- `<interface-type>` - Displays the flow-control information for the specified type of interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.

    - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
    - extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
- <interface-id> - Displays the flow-control information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.

Mode Privileged EXEC Mode

Note: If this command is executed without the optional parameter it displays the flowcontrol information of the switch. Otherwise it displays the flowcontrol information of the specified interface.

Example

```
Your product# show flow-control interface gigabitethernet 0/2
Port Tx                  FlowControl     Rx Flow Control     Tx Pause     Rx Pause     HC
TxPause                  HC RxPause      ---------------     --------     --------     --
                         ---------------------------------   -----------  ----------

Gi0/2                    on        on    0                   0            0            0
```

Related Command(s)

- show interfaces - Displays interface status and configuration
- flowcontrol - Enables flowcontrol on an interface

show debug-logging

Command Objective This command displays the debug logs stored in file.

Syntax **show debug-logging**

Mode Privileged EXEC Mode

Example

```
Your Product(config)# debug-logging file
Your Product(config)# exit
Your product# debug spanning-tree events
Your product# show debug-logging
AST: AST:
AST:       MSG: MSG:
MSG:       Timer Expiry Event processed... Completed processing the
event(s).
Timer Expiry Event processed...
AST:       MSG:     Completed processing the event(s).
AST:       MSG:     Timer Expiry Event processed...
AST:
```

```
AST:        MSG:

MSG:        Completed processing the event(s).

Timer Expiry Event processed...
AST:        MSG:     Completed processing the event(s).
AST: AST:
AST:        MSG: MSG:
MSG:        Timer Expiry Event processed... Completed processing the
event(s).
Timer Expiry Event processed...
AST:

AST:        MSG:

MSG:        Completed processing the event(s).

Timer Expiry Event processed...
AST:        MSG:     Completed processing the event(s).
AST:

AST:        MSG:

MSG:        Timer Expiry Event processed...

Completed processing the event(s).
AST:        MSG:     Timer Expiry Event processed...
AST:        MSG:     Completed processing the event(s).
```

Related Command(s) `debug-logging` - Configures where debug logs are to be displayed

show debugging

Command Objective This command displays state of each debugging option.

Syntax **show debugging**

Mode Privileged EXEC Mode

Example

```
Your product# show debugging
Spanning Tree:
Spanning tree timers related debugging is on
```

Related Command(s)

- `debug spanning-tree` - Provides spanning tree debugging support
- `debug dot1x` - Enables debugging of dot1x module
- `debug radius` - Enables RADIUS debugging options
- `debug ip igmp snooping`- Specifies the debug levels for the IGMP snooping module
- `debug ssh` - Sets the given trace levels for SSH

- `debug ssl` - Sets the given debug levels for SSL
- `debug vlan`- Enables the tracing of the VLAN submodule as per the configured debug levels.
- `debug garp`- Enables the tracing of the GARP submodule as per the configured debug levels.
- `debug ip dhcp client` - Enables the tracking of the DHCP client operations as per the configured debug levels.
- `debug ip dhcp relay`- Enables the debug level for tracing the DHCP Relay Module
- `debug ip dhcp server`- Enables the tracking of the DHCP server operations as per the configured debug levels.

show clock

Command Objective This command displays the system date and time.

Syntax **show clock**

Mode Privileged EXEC Mode

Example

```
Your product# show clock
Fri Jun 28 08:31:19 2013 (UTC +05:50)
```

Related Command(s) `clock set` - Manages the system clock

show running-config

Command Objective This command displays the configuration information currently running on the switch, the configuration for a specific interface, or map class information and this configuration is lost if the system is restarted The command is useful when there are multiple interfaces and you want to look at the configuration of a specific interface.

Syntax **show running-config [{ syslog | dhcp | dhcp6 | dvmrp | |stp [switch <context_name>] | ecfm [switch<context_name>] | la | pnac | igs | mlds | vlan <vlan- id/vfi-id> [switch <context_name>] | interface {<interfacetype> <interfacenum> | vlan <vlan-id/vfi-id>} | ospf | isis | rip | bgp | ipv6 | rip6 | ssh | ssl | acl | ip | pim | pimv6 | vrrp | snmp | radius | rmon | rm | mbsm | ospf3 | mpls | igmp | eoam | fm | igmp-proxy | elmi | route-map | tacacs | tac | sntp | switch <context_name> | nat | elps | erps | [switch <context_name>] | entity-mib | http | poe | pbb [switch <context_name>] |cn [switch<context_name>] | dcbx | ptp |clkiwf | mld | msdp | msdpv6 | lldp | firewall | system | ospfte | ipsourceguard | tlm | rbridge | l2dhcsnp | mef | network-clock | vrf <vrf- name> | hs | bfd | qosxtd | dsmon | mrp | ofc}]**

Parameter Description

- `syslog` - Displays the configuration done in the syslog module.
- `dhcp` - Displays the configuration done in the DHCP module.

- `dvmrp` - Displays the configuration done in the DVMRP module.
- `stp` - Displays the configuration done in the STP module.
  - `switch <context_name>` - Displays the configuration done in the context for the specified module. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
- `ecfm` - Displays the configuration done in the ECFM module.
- `la` - Displays the configuration done in the LA module.
- `pnac` - Displays the configuration done in the PNAC module.
- `igs` - Displays the configuration done in the IGS module.
- `mlds` - Displays the configuration done in the MLDS module.
- `vlan <vlan-id/vfi-id>` - Displays the configuration done for the specified VLAN / VFI ID. This is a unique value that represents the specific VLAN/ VFI created / to be created. This value ranges between 1 and 65535.
  - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - `<vfi-id>.` - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

    Notes:

    - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
    - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
    - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
  - `switch <context_name>` - Displays the configuration done in the context for the specified module. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
- `interface` - Displays the configuration done for the specified type of interface
  - `<interfacetype>` - Displays the configuration done for the specified type of interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabit per second. This Ethernet supports only full duplex links
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `port-channel` – Logical interface that represents an aggregator which contains several

ports aggregated together.

  - `<interface-id>` - Displays the configuration done for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.
  - `vlan <vlan-id/vfi-id>` - Displays the configuration done for the specified VLAN / VFI ID. This is a unique value that represents the specific VLAN/ VFI created / to be created. This value ranges between 1 and 65535.
  - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - `<vfi-id>`. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

  Notes:

  - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
  - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
  - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- `ospf` - Displays the configuration done in the OSPF module.
- `rip` - Displays the configuration done in the RIP module.
- `bgp` - Displays the configuration done in the BGP module.
- `ipv6` - Displays the configuration done in the IPv6 module.
- `rip6` - Displays the configuration done in the RIP6 module.
- `ssh` - Displays the configuration done in the SSH module.
- `ssl` - Displays the configuration done in the SSL module.
- `acl` - Displays the configuration done in the ACL module.
- `ip` - Displays the configuration done in the IP module.
- `pim` - Displays the configuration done in the PIM module.
- `vrrp` - Displays the configuration done in the VRRP module.
- `snmp` - Displays the configuration done in the SNMP module.
- `radius` - Displays the configuration done in the RADIUS module.
- `rmon` - Displays the configuration done in the RMON module.
- `rm` - Displays the configuration done in the RM module.
- `mbsm` - Displays the configuration done in the MBSM module.
- `ospf3` - Displays the configuration done in the OSPFv3 module.
- `mpls` - Displays the configuration done in the MPLS module.
- `igmp` - Displays the configuration done in the IGMP module.

- eoam - Displays the configuration done in the EOAM module.
- fm - Displays the configuration done in the FM module.
- igmp-proxy - Displays the configuration done in the IGMP proxy module.
- elmi - Displays the configuration done in the ELMI module.
- route-map - Displays the configuration done for the route map feature.
- tacacs - Displays the configuration done in the TACACS module.
- tac - Displays the configuration done in the TAC module.
- sntp - Displays the configuration done in the SNTP module.
- switch <context_name> - Displays the configuration done in the context for the specified module. **Note:** This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
- nat - Displays the configuration done in the NAT module.
- elps - Displays the configuration done in the ELPS module.
- erps - Displays the configuration done in the ERPS module.
- switch <context_name> - Displays the configuration done in the context for the specified module. **Note:** This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
- entity-mib - Displays the configuration done in the emtity-mib module.
- http - Displays the configuration done in the http module.
- poe - Displays the configuration done in the poe module.
- pbb - Displays the configuration done in the pbb module.
- switch <context_name> - Displays the configuration done in the context for the specified module. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
- cn - Displays the configuration done in the cn module.
- switch <context_name> - Displays the configuration done in the context for the specified module. **Note:** This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
- dcbx - Displays the configuration done in the extended dcbx module.
- ptp - Displays the configuration done in the ptp module.
- clkiwf - Displays the configuration done in the clkiwf module.
- mld - Displays the configuration done in the mld module.
- msdp - Displays the configuration done in the msdp module.
- msdpv6 - Displays the configuration done in the msdpv6 module.
- lldp - Displays the configuration done in the lldp module.
- firewall - Displays the configuration done in the firewall module.
- system - Displays the configuration done in the system.
- ospfte - Displays the configuration done in the OSPF TE module.
- ipsourceguard - Displays the configuration done in the IP Source Guard module.
- tlm - Displays the configuration done in the TLM module.
- rbridge - Displays the configuration done in the Rbridge module.
- l2dhcsnp - Displays the configuration done in L2 DHCP snooping module.
- mef - Displays the configuration done in MEF module

- `network-clock` - Displays the configuration done in SyncE module
- `vrf <vrf-name>` - Displays the configuration done for the specified VRF instance created in the system.
- `hs` - Displays the configuration done in HotSpot module
- `bfd` - Displays the configuration done in BFD module
- `qosxtd` - Displays the configuration done in QoSx module
- `qosx` - Displays the configuration done in QoS module
- `dsmon` - Displays the configuration done in DSMON module
- `mrp` - Displays the configuration done in MRP module
- `ofc` - Displays the configuration done in OFCL module

Mode Privileged EXEC Mode

Note: If executed without the optional parameters this command displays the current active configurations, other than the default configurations of all the modules in all the interfaces. Not all the features are supported at all SMIS models.

Example The output given below is only a fragment of the whole output. This output differs based on the modules that are configured.

```
Your product# show running-config stp
Building configuration... spanning-tree mode rst interface gigabitethernet
0/1! interface gigabitethernet 0/2! interface gigabitethernet 0/3!
interface gigabitethernet 0/4! interface gigabitethernet 0/5! interface
gigabitethernet 0/6! interface gigabitethernet 0/7! interface
gigabitethernet 0/8! interface gigabitethernet 0/9! interface
gigabitethernet 0/10! interface gigabitethernet 0/11! interface
gigabitethernet 0/12!
interface gigabitethernet 0/13!
interface gigabitethernet 0/14!
interface gigabitethernet 0/15! interface gigabitethernet 0/16! interface
gigabitethernet 0/17! interface gigabitethernet 0/18! interface
gigabitethernet 0/19! interface gigabitethernet 0/20! interface
gigabitethernet 0/21! interface gigabitethernet 0/22! interface
gigabitethernet 0/23! interface gigabitethernet 0/24! end
Your product# show running-config bgp
Building configuration... router bgp 100
bgp router-id 100.20.6.100
bgp default ipv4-unicast
redistribute static
restart-reason softwareRestart
 neighbor      100.20.6.20   remote-as 200
 neighbor      100.20.6.20   update-source 100.20.6.100
 neighbor      100.20.6.20   timers holdtime 240
 neighbor      110.20.6.20   remote-as 300
 neighbor      110.20.6.20   update-source 110.20.6.100
 neighbor  end 110.20.6.20   timers holdtime 240!
```

Related Command(s) Related Command include the configuration commands of all the modules (given as parameters in the show running-config command)

show http server status

Command Objective This command displays the http server status and HTTP port.

Syntax s **how http server status**

Mode Privileged EXEC Mode

Example

```
Your product# show http server status
HTTP server status              : Enabled
HTTP port is                    : 80
HTTP Requests In                : 0
HTTP Invalids                   : 0
```

Related Command(s)

- `ip http port` – Sets the HTTP port
- `set ip http` – Enables/disables HTTP

show system acknowledgement

Command Objective This command displays acknowledgement statement for open sources used in the software.

Syntax **show system acknowledgement**

Mode Privileged EXEC Mode

Example `Your product# show system acknowledgement`

Notes:

- The SSH functionality in this switch is implemented using the open source software from http://www.openssh.org developed by Theo de Raadt, Niels Provos, Markus Friedl, Bob Beck, Aaron Campbell and Dug Song. All copyrights listed at http://www.openssh.org apply.
- The SSL functionality in this switch is implemented using the open source software from http://www.openssl.org which include software written by Er.c A. Young and Tim J. Hudson.All copyrights listed at http://www.openssl.org apply.
- This switch includes cryptographic software written by Eric A Young (eay@cryptsoft.com). This product includes software written by Tim J. Hudson (tjh@cryptsoft.com). PLEASE REMEMBER THAT EXPORT/IMPORT AND/OR USE OF STRONG CRYPTOGRAPHY SOFTWARE, PROVIDING CRYPTOGRAPHY HOOKS OR EVEN JUST COMMUNICATING TECHNICAL DETAILS ABOUT CRYPTOGRAPHY SOFTWARE IS ILLEGAL IN SOME PARTS OF THE WORLD. SO, WHEN YOU IMPORT THIS PACKAGE TO

YOUR COUNTRY, RE-DISTRIBUTE IT FROM THERE OR EVEN JUST EMAIL TECHNICAL SUGGESTIONS OR EVEN SOURCE PATCHES TO THE AUTHOR OR OTHER PEOPLE YOU ARE STRONGLY ADVISED TO PAY CLOSE ATTENTION TO ANY

- EXPORT/IMPORT AND/OR USE LAWS WHICH APPLY TO YOU. THE AUTHORS OF OPENSSL ARE NOT LIABLE FOR ANY VIOLATIONS YOU MAKE HERE. SO BE CAREFUL, IT IS YOUR RESPONSIBILITY
- Math library in this switch is implemented using the Open source software from Sun Microsystems, Inc. All copyrights listed at http://www.radiks.net/~rhuebner/mathlib.html apply.
- Web Tree View Script (ftiens4.js) and Browser Detection Script (ua.js) in this switch are implemented using source code from http://www.treeview.net. All copyright listed at http://www.treeview.net apply.

show mac-learn-rate

Command Objective This command displays maximum number of unicast dynamic MAC (L2) MAC entries hardware can learn on the system, in MAC learning limit rate interval. mac-learn-rate is not supported on some SMIS models.

Syntax **show mac-learn-rate**

Mode Privileged EXEC mode

Example

```
Your product# show mac-learn-rate
Switch MAC Learn Limit Rate : 1000
Switch MAC Learn Limit Rate Interval: 1000
```

Related Command(s) `mac-learn-rate` - Configures the number of MAC entries indication to control plane from hardware, when hardware MAC learning is enabled.

port-isolation in_vlan_ID

Command Objective This command enables the VLAN traffic to be allowed in these configured egress ports when the ingress is this interface.

The no form of the command disables the Port Isolation rule in this ingress interface.

Syntax **port-isolation in_vlan_ID [{add|remove}]**
port_list no port-isolation

Parameter Description

- `in_vlan_ID` - Configures the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
- `add` - Configures the addition of the egress ports

- `remove` - Configures the removal of the egress ports
- `port_list` - Configures the list of ports through which the traffic is allowed. The ports can be either a physical or link aggregated port.

Mode Interface configuration mode (physical ports or Link Aggregated port).

Example `Your Product(config-if)# port-isolation 4094 add Gi0/1-10`

Related Command(s) `show port-isolation` - Displays the Port Isolation table

show port-isolation

Command Objective This command displays the Port Isolation table.

Syntax **show port-isolation [ingress-port <ifXtype> <ifnum>]**

Parameter Description

- `ingress-port` - Ingress port refers to a physical or link aggregated port through which a packet ingress.
  - `<ifXtype>`– Displays the type of interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `port- channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
  - `<ifnum>` Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash.

Mode Privileged EXEC Mode

Example

```
Your product# show port isolation
Ingress Port        VlanId       StorageType         Egress List
============        ======       ===========         ===========
Gi0/2               10           Non-Volatile        Gi0/1
Gi0/3               -            Non-Volatile        Gi0/2
```

Related Command(s): `port-isolation in_vlan_ID` - Enables the VLAN traffic to be allowed in these configured egress ports when the ingress is this interface.

private-vlan mapping

Command Objective This command maps list of secondary VLAN to the primary VLAN IVR interface, so that secondary VLANs can use the primary VLAN IVR interface for L3 communication.

The no form of the command removes all secondary VLAN association to the primary VLAN IVR interface.

Note: This command is not supported in all models.

Syntax **private-vlan mapping [{add | remove}] <vlan-list> no private-vlan mapping**

Parameter Description

- `add` - Maps the list of configured secondary VLAN to the existing primary VLAN IVR interface
- `remove` - Removes the mapping between the secondary VLAN and the primary VLAN IVR interface
- `<vlan-list>` - Configures a VLAN ID or list of VLAN IDs that should be mapped with the specified primary VLAN. For example, the value is provided as 5, 6, or 7 to represent the list of VLANs IDs. Specifies the VLAN list for the private VLAN interface. All existing mapped secondary VLANs will be deleted.

Mode Interface Configuration Mode

Example

```
Your Product (config-if)# private-vlan mapping 18
```

Related Command(s) `show interfaces` - Displays the interface status and configuration.

audit-logging

Command Objective This command enables or disables audit logging that allows users to configure audit trails, which track changes that have been made to a router. Each change is logged as a syslog message, and all syslog messages are kept in the audit file, which is kept in the audit subsystem.

Syntax **audit-logging { enable | disable}**

Parameter Description

Default `disable` - Disables audit logging.

Mode Global Configuration Mode

Related Command(s)

- `audit-logging filename` - Specifies the name of the file to which Audit log is saved
- `audit-logging filesize` - Specifies the maximum file size in Kilobytes of the configs.txt file
- `audit-logging reset` - Erases the contents in configs.txt file and start logging
- `show confg log` - Displays Information related to Audit Logging

audit-logging filename

Command Objective This command specifies the name of the file to which Audit log is saved. The maximum string value of the file name is 128.

Syntax **audit-logging filename <filename>**

Mode Global Configuration Mode

Default Config.txt

Example

```
Your Product(config)# audit-logging filename srv.txt
```

Related Command(s)

- `audit-logging` – Enables/disables audit logging
- `audit-logging filesize` - Specifies the the maximum file size in Kilobytes of the configs.txt file
- `audit-logging reset` - Erases the contents in configs.txt file and start logging
- `show confg log` - Displays Information related to Audit Logging

audit-logging filesize

Command Objective This command specifies the maximum file size (in Kilobytes of the configs.txt file) of the audit file which is a fixed file size in the disk file system. The audit file contains syslog messages and it is stored on the disk. The number of messages that can be stored is dependent on the size of the selected file and the size determines the number of messages that can be stored on the disk before a wraparound occurs. Ensure that the audit file is secure and the audit file should be access protected so that only the audit subsystem can access it. The value ranges between 1024 and 1048576.

Syntax **audit-logging filesize <filesize(1024-1048576)>**

Mode Global Configuration Mode

Default 1048576

Example

```
Your Product(config)# audit-logging filesize 1025
```

Related Command(s)

- `audit-logging` – Enables/disables audit logging
- `audit-logging filename` - Specifies the name of the file to which Audit log is saved
- `audit-logging reset` - Erases the contents in configs.txt file and start logging
- `show confg log` - Displays Information related to Audit Logging

audit-logging reset

Command Objective This command is used to erase the contents in configs.txt file and start logging.

Syntax **audit-logging reset**

Mode Global Configuration Mode

Example

```
Your Product(config)# audit-logging reset
```

Related Command(s)

- `audit-logging` – Enables/disables audit logging
- `audit-logging filesize` - Specifies the maximum file size in Kilobytes of the configs.txt file
- `audit-logging filename` - Specifies the name of the file to which Audit log is saved
- `show confg log` - Displays Information related to Audit Logging

show config log

Command Objective This command displays Information related to Audit Logging.

Syntax **show config log**

Mode Privileged EXEC Mode

Example

```
Your product# show config log Audit Status    : Enabled Audit File Name : config.text
Audit File Size  : 1025
Audit Log Size Threshold : 70
```

Related Command(s)

- `audit-logging` – Enables/disables audit logging
- `audit-logging filename` - Specifies the name of the file to which Audit log is saved
- `audit-logging filesize` - Specifies the maximum file size in Kilobytes of the configs.txt file
- `audit-logging reset` - Erases the contents in configs.txt file and start logging

hol blocking prevention

Command Objective This command enables or disable the Head-of-Line Blocking prevention which manages the HOL blocking situation by checking whether the packet has been assigned priority, if the packets have assigned priority, those packets are placed in a separate queue. The low priority data can be discarded as applications keep track of whether a retransmission is necessary or not

Note: This command is not supported in MBM-XEM-002

Syntax **hol blocking prevention**

Mode Global Configuration Mode

Example `Your product# hol blocking prevention`

internal-lan

Command Objective This command adds an internal lan interface and its parameters

Syntax **internal-lan <ilan-id (1-65535)> {add interface virtual <iface_list> | delete interface virtual <iface_list>}**

Parameter Description

- `<ilan-id (1-65535)>` - Specifies the internal LAN id. The value ranges between 1 to 65535
- `add interface virtual <iface_list>` - Adds the internal LAN interface and its parameters. Specifies the virtual interface
- `delete interface virtual <iface_list>` - Deletes the internal LAN interface and its parameters. Specifies the virtual interface.

Mode Global Configuration Mode

Example `Your Product(config)# internal-lan 1 add interface virtual 0/1`

Related Command(s) `show internal-lan` - Displays the internal LAN parameters.

show internal-lan

Command Objective This command displays the internal LAN parameters.

Syntax **show internal-lan <iface_list>**

Mode Privileged EXEC Mode

Example `Your product# show internal-lan`

Related Command(s) `internal-lan`- Adds an ilan interface and its parameters

show iftype protocol deny table

Command Objective This command displays the entries of iftype protocol deny table.

Syntax **show iftype protocol deny table [switch <context_name>]**

Parameter Description `switch <context_name>`- Displays iftype for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example `Your Product# show iftype protocol deny table`

Related Command(s) `deny iftype` - Denies the particular type of interface, bridge ports in the given protocol module, from being accessed by the protocol

clear line vty

Command Objective This command clears the console or virtual terminal line to an idle state.

Syntax **clear line vty {<line-number(2-9)> | all}**

Parameter Description

- `<line-number(2-9)>` - Clears the vty information of the specified telnet session. This value ranges between 2 and 9.
- `all` - Clears all the vty information.

Mode Privileged EXEC Mode

Example

```
Your Product# clear line vty 2
```

Related Command(s) `show line` ---Displays the TTY line information

tunnel hop-limit

Command Objective This command configures Hop Limit on Tunnel. The hop limit value ranges between 0 and 255.

Syntax **tunnel hop-limit <0-255>**

Mode Interface configuration mode (Tunnel)

Note: This command executes only if the tunnel interface is configured

Example

```
Your Product(config)# interface tunnel 1
Your Product(config-if)# tunnel mode ipv6ip config-id 1 source vlan1 dest
10.203.113.114
Your Product(config-if)# tunnel hop-limit 5
```

Related Command(s) `tunnel mode` - Configures the tunnel interface with the associated parameters

login block-for

Command Objective This command configures the maximum number of successful login attempts and the lock out time to block the user.

Syntax **login block-for <seconds(30-600)> attempts <tries(1-10)>**

Parameter Description

- `<seconds(30-600)>` - Configures the lock out time in seconds that a user is blocked following unsuccessful logins. This value ranges between 30 and 600.
- `<tries(1-10)>` - Configures login attempts. This is the number of times a user is allowed to login using wrong password in the login prompt. This value ranges between 1 and 10.

Mode Global Configuration mode

Default

- `seconds` - 30
- `tries` – 3

Example

```
Your Product(config)# login block-for 30 attempts 3
```

audit-logging logsize-threshold

Command Objective This command configures the threshold value of the log storage space with respect to the maximum storage space size. The threshold value in percentage ranges between 1 and 99.

Syntax **audit-logging logsize-threshold <threshold in %(1-99)>**

Mode Global Configuration mode

Default threshold in % - 70

Example

```
Your Product(config)# audit-logging logsize-threshold 99
```

Related Command(s) `show config log` - Displays the information related to Audit Logging.

feature telnet

Command Objective This command enables the telnet service in the system.

The no form of this command disables the telnet service.

Syntax **feature telneto feature telnet n**

Mode Global Configuration mode

Default The telnet service is enabled

Example

```
Your Product(config)# feature telnet
```

Related Command(s) `show telnet server` - Displays the telnet server status.

show telnet server

Command Objective This command displays the telnet server status.

Syntax **show telnet server**

Mode Privileged EXEC Mode

Example

```
Your Product# show telnet server
telnet service enabled
```

Related Command(s) `feature telnet` - Enables the telnet service in the system.

show audit

Command Objective This command displays the content of the audit-log file.

Syntax **show audit**

Mode Privileged EXEC Mode

Example

```
Your Product# show audit
Audit:ADMIN audi-t logging reset21:27:54 2011
Audit:ADMIN firewall SUCCESS CONSOLE Fri Jun 10 21:27:57
2011
Audit:ADMIN enable SUCCESS CONSOLE Fri Jun 10 21:27:58 2011
Audit:ADMIN end SUCCESS CONSOLE Fri Jun 10 21:28:01 2011
Audit:ADMIN c t SUCCESS CONSOLE Fri Jun 10 21:28:04 2011
Audit:ADMIN enable password level 5 Password123$ SUCCESS CONSOLE Fri Jun 10
21:28:45 2011
Audit:ADMIN end SUCCESS CONSOLE Fri Jun 10 21:28:46 2011
```

set http authentication-scheme

Command Objective This command configures the Configurable HTTP authentication scheme.

Syntax **set http authentication-scheme {default | basic | digest}**

Parameter Description

- `default` - Sets the configurable HTTP authentication scheme to default.
- `basic` - Sets the configurable HTTP authentication scheme to basic.
- `digest` - Sets the configurable HTTP authentication scheme to digest.

Mode Global Configuration Mode

Default default

Example

```
Your Product (config)# set http authentication-scheme basic
```

Related Command(s) `show http authentication-scheme` - Displays the Operational and Configurable authentication scheme values.

set http redirection enable

Command Objective This command enables the HTTP redirection feature.

The no form of this command disables the HTTP redirection feature.

Syntax **set http redirection enable no http redirection enable**

Mode Global Configuration Mode

Default HTTP redirection is disabled

Example

```
Your Product (config)# set http redirection enable
```

http redirect

Command Objective This command configures the alternate server for the URL specified. The alternate server's IP or Domain name can be specified. On receiving request for the URL, a redirection status is sent as response for the request.

The no form of this command removes the redirection entry added to the server specified for the URL.

Syntax **http redirect <URL to be redirected> server {IPv4 Address |IPv6 Address | Domain name}**
no http redirect [<URL to be redirected>]

Parameter Description

- `<URL to be redirected>` - Configures the URL which has to be redirected.
- `server` - Configures the server for the URL which is redirected. The options are:
- `IPv4 Address` – Sets the IP address of the alternate server in v4 format
- `IPv6 Address` – Sets the IP address of the alternate server in v6 format
- `Domain name` - Configures the domain name of the alternate server

Mode Global Configuration Mode

Example

```
Your Product (config)# http redirect /sample/ server
12.0.0.2
```

Related Command(s) `show http redirection` - Displays the redirection entries filtered by URL or all the entries.

show http authentication-scheme

Command Objective This command displays the operational and configurable authentication scheme values.

Syntax **show http authentication-scheme**

Mode Privileged EXEC Mode

Example

```
Your Product# show http authentication-scheme
The Operational HTTP authentication scheme is Digest
The Configured HTTP authentication scheme is Digest
```

Related Command(s) `set http authentication-scheme` – Sets the Configurable HTTP Authentication scheme value to default or basic or digest.

show http redirection

Command Objective This command displays the redirection entries filtered by URL or all the entries.

Syntax **show http redirection [URL]**

Parameter Description `URL` - Configures the URL for which the redirection entry has to be displayed.

Mode Privileged EXEC Mode

Example

```
Your Product# show http redirection /sample/
HTTP Redirection Entries
-------------------------------------------
URL                           Server IP/DomainName
---                           --------------------
/sample/                      12.0.0.2
```

Related Command(s) `http redirect` - Configures the alternate server for the URL specified.

4.1ENTITY MIB

Entity MIB is a standardized way of representing a single agent, which supports multiple instances of one MIB. With the Entity MIB support in SMIS, all the instances of the MIBs registered with agent are identifiable, so that the NMS (Network Management System) can easily communicate with the particular instance / logical entity. Entity MIB also provides the complete hierarchal hardware component view to the user.

The list of CLI commands for the configuration of ENTITY MIB is as follows:

- set entity physical-index
- show entity logical

- show entity physical
- show entity lp-mapping
- show entity alias-mapping
- show entity phy-containment

set entity physical-index

Command Objective This command configures the read-write objects of the physical components present in the system which defines a greater than zero value used to identify a physical entity. The physical index is an arbitrary value that uniquely identifies the physical entity which can be small positive integer.

Syntax **set entity physical-index <integer (1..2147483647)>{[asset-id <SnmpAdminString (Size (1..32))>] [serial-number <SnmpAdminString (Size (1..32))>] [alias-name <SnmpAdminString (Size (1..32))>] [uris <OCTET-STRING (Size(1..255))>]}**

no entity physical-index <integer (1-2147483647)> [assetId] [serial-number][alias-name][uris]

Parameter Description

- <integer(1..2147483647)> - Specifies the Index of the physical entity. The value ranges between 1 and 2147483647.
- asset-id - Specifies the asset tracking identifier for the physical entity.

  Note: This value is a string of size varying between 1 and 32 characters. Asset tracking identifier is not needed for the physical entities (such as repeater ports within a repeater module) that are not considered as a field replaceable unit by the vendor. A zero-length string is returned for these entities.

- serial-number - Specifies the vendor-specific serial number string for the physical entity. This value is a string of size varying between 1 and 32 characters. Serial number string is not needed for the physical entities (such as repeater ports within a repeater module) that are not considered as a field replaceable unit by the vendor. A zero-length string is returned for these entities.
- alias-name - Specifies the alias name for the physical entity. This value provides a non-volatile handle for the entity. This value is a string of size varying between 1 and 32 characters.
- uris - Specifies the additional identification information (that is URI (Uniform Resource Indicator) about the physical entity. This value ranges between 1 and 255.

Mode Global Configuration mode

Default

- `assetId` - Zero-length string, on initial instantiation of the physical entity.
- `serial-number` - Zero-length string, on initial instantiation of the physical entity, if a serial number is unknown or non-existent. Correct vendor- assigned serial number, on initial instantiation of the

physical entity, if the serial number is available to the SNMP agent.

- `alias-name` - Zero-length string, on initial instantiation of the physical entity. The SNMP agent may also set the value to a locally unique default value.

Notes:

- If write access is implemented for an instance of asset ID and a value is written into the instance, SNMP agent should retain the value as long as the entity associated with the instance remains instantiated. This instantiation includes the instantiation across all re-initialization / reboot of the NMS. and instantiation resulting in a change of the physical entity's index value.
- If write access is implemented for an instance of the serial number string and a value is written into the instance, SNMP agent should retain the value as long as the entity associated with the instance remains instantiated. This instantiation includes the instantiation across all re-initialization / reboot of the NMS. and instantiation resulting in a change of the physical entity's index value.
- If the agents cannot provide non-volatile storage for the serial number string, then the agents are not required to implement write access for the the serial number string object.
- Implementations that can correctly identify the serial numbers of all installed physical entities are not required to provide write access to the serial number string object
- If write access is implemented for an instance of the alias name and a value is written into the instance, SNMP agent should retain the value as long as the entity associated with the instance remains instantiated. This instantiation includes the instantiation across all re-initialization / reboot of the NMS. and instantiation resulting in a change of the physical entity's index value.

Example

```
Your Product(config)# set entity physical-index 2222222 asset-id 8 serial-number 7 alias-name GJG uris yg
```

Related Command(s) `show entity physical` - Displays the physical entities

show entity logical

Command Objective This command displays multiple logical entities within a single physical entity. The overall physical entity contains multiple (smaller) physical entities and each logical entity is associated with a particular physical entity.

Syntax **show entity logical [index <integer (1..2147483647)>]**

Parameter Description `index<integer (1..2147483647)>` - Displays the index of the logical entity. The value ranges between 1 and 2147483647.

Mode Privileged EXEC Mode

Example

```
Your product# show entity logical index 1
Logical Index: 1
Logical Description: SMIS Logical Type: stdpnac Logical Community: default
Logical Transport Address: Logical Transport Domain:
Logical Context Engine Id: 80:00:08:1c:04:46:64
Logical Context Name: default
```

Related Command(s) `set entity physical-index`- Configures the read-write objects of the physical components present in the system.

show entity physical

Command Objective This command displays the physical entities which are physical components that represents an identifiable physical resource within a managed system. Zero or more logical entities may utilize a physical resource at any given time.

Syntax **show entity physical [index <integer (1..2147483647)>]**

Parameter Description `index<integer (1..2147483647)>`- Displays the index of the physical entity. The value ranges between 1 and 2147483647.

Mode Privileged EXEC Mode

Example

```
Your product# show entity physical index 1
Physical Index: 1
Physical Descr: Network Element Physical VendorType: Supermicro Physical
ContainedIn: 0
Physical Class: 3
Physical ParentRelPos: 0
Physical Name: SMIS
Physical HardwareRev: 1.0.2
Physical SoftwareRev: 2.0.0
Physical FirmwareRev: 2.0.0
Physical Serial Num: MBM-XEM-002
Physical MfgName: Supermciro
Physical ModelName: Physical Alias: DummyName Physical AssetID: assetId
Physical MfgDate: 2009-8-6,13:30:30.0,-4:0
Physical Uris:
Physical FRU Status: 1
```

Related Command(s)

- `interface-configuration and deletion` - Configures interface such as out of band management, port channel, tunnel and so on.
- `set entity physical-index` - Configures the read-write objects of the physical components present in the system

show entity lp-mapping

Command Objective This command displays the mapping of logical and physical entities, interfaces, and non-interface ports managed by a single agent. The LPMapping contains mappings between logical entities and physical components supporting that entity. A logical entity can map to more than one physical component, and more than one logical entity can map to the same physical component.

Syntax **show entity lp-mapping**

Mode Privileged EXEC Mode

Example

```
Your product# show entity lp-mapping
Logical Index - 1 is mapped to Physical Index- 10
Logical Index - 1 is mapped to Physical Index- 11
Logical Index - 2 is mapped to Physical Index- 10
Logical Index - 2 is mapped to Physical Index- 11
Logical Index -3 is mapped to Physical Index-10
```

Related Command(s) `map switch` - Maps the port to the Context

show entity alias-mapping

Command Objective This command displays the mapping of logical and physical entity with alias external object identifiers values. This allows resources managed with other MIBs (e.g. repeater ports, bridge ports, physical and logical interfaces) to be identified in the physical entity hierarchy. Each alias identifier is only relevant in a particular naming scope.

Syntax **show entity alias-mapping [index <integer (1..2147483647)>]**

Parameter Description `index <integer (1..2147483647)>`- Displays the Index of the physical entity. The value ranges between 1 and 2147483647.

Mode Privileged EXEC Mode

Example

```
Your product# show entity alias-mapping
Physical Index -10 for all Logical entities is mapped to external identifier : Gi0/1
Physical Index - 11 for all Logical entities is mapped to external identifier : Gi0/24
```

Related Command(s) `interface`– configuration and deletion - Configures interface such as out of band management, port channel, tunnel and so on.

show entity phy-containment

Command Objective This command displays the simple mapping between the physical contained values for each container/containee relationship in the managed system.

Syntax **show entity phy-containment [index <integer (1..2147483647)>]**

Parameter Description `index <integer (1..2147483647)>`- Displays the Index of the physical entity. The value ranges between 1 and 2147483647.

Mode Privileged EXEC Mode

Example

```
Your product# show entity phy-containment
Containmaint Relationship
Physical Entity            :      1 (Chassis)
Member Physical Entities:         2 (Cpu), 3 (Power Supply), 4 (Fan)
                                  5 (Fan), 6 (Fan), 7 (Fan)
                                  8 (Fan), 9 (Module)

Physical Entity                   :9     (Module)
Member Physical Entities:         10     (Port),      11     (Port),      12     (Port)
                                  13     (Port),      14     (Port),      15     (Port)
                                  16     (Port),      17     (Port),      18     (Port)
                                  19     (Port),      20     (Port),      21     (Port)
                                  22     (Port),      23     (Port),      24     (Port)
                                  25     (Port),      26     (Port),      27     (Port)
                                  28     (Port),      29     (Port),      30     (Port)
                                  31     (Port),      32     (Port),      33     (Port)
```

Related Command(s) `interface – configuration and deletion` - Configures interface such as out of band management, port channel, tunnel and so on.

set hitless-restart enable

Command Objective This command enables the hitless restart feature by which the software is restarted without affecting any datapath and without disturbing the protocol relationships with any peer nodes. This command is not supported.

Syntax **set hitless-restart enable**

Mode Privileged EXEC Mode

Default Hitless restart is disabled.

Example

```
Your Product# set hitless-restart enable
<129>Nov 9 04:54:50 SMIS FM [FM - RM] : 131.0.0.1
RM :ACTIVE completed started none :: Nov 9 04:54:49
2011
SMIS# Nov 9 04:54:49 2011: RM[ACTIVE]:
Hitless Restart: Bulk storage completed.Nov 9 04:54:49
2011: RM[ACTIVE]:
Hitless Restart: Steady state pkt request starts. Nov9 04:54:49 2011:
RM[ACTIVE]:
Hitless Restart: All Steady State packets are stored in
```

```
NPSIM.Nov 9 04:54:49 2011: RM[ACTIVE]:
Do write start-up and PLEASE RESTART THE EXE
```

speed

Command Objective This command sets the speed of the interface.

Syntax **speed { 10 | 100 | 1000 | 10000 | 40000 | 56000 | auto |nonegotiate}**

Parameter Description

- `10` - Sets the port to run at 10Mbps.
- `100` - Sets the port to run at 100Mbps.
- `1000` - Sets the port to run at 1000Mbps.
- `10000` - Sets the port to run at 10000Mbps.
- `40000` - Sets the port to run at 40000Mbps.
- `56000` - Sets the port to run at 56000Mbps.
- `auto` - Detects and sets the speed of the port automatically based on the peer switch.
- `nonegotiate` - Disables negotiation on the ports.

Mode Interface Configuration Mode

Example

```
Your Product(config-if)# speed 10
```

automatic-port-create

Command Objective This command enables or disables the Automatic Port Create feature. This configuration takes effect only after system restart.

Note: To create or delete ports at STP module level, the Automatic Port Create feature has to be disabled.

Syntax **automatic-port-create { enable | disable }**

Parameter Description

- `enable` - Enables Automatic Port Create feature and the ports are automatically created in STP module when it is mapped to a context.
- `disable` - Disables Automatic Port Create feature. When set to disabled, ports are not created automatically and ports can be created at STP.

Mode Global Configuration Mode

Default enable

Example

```
Your Product(config)# automatic-port-create enable
```

Related Command(s)

- `spanning-tree` - Properties of an interface - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.

- `show nvram` - Displays the current information stored in the NVRAM.
- `write start-up config` - Writes the running-config to a flash file, startup-configuration file or to a remote site

port-type providerInstancePort

Command Objective This command configures the PIP (Provider Instance Port) type. PIP is nothing but a Backbone Edge Bridge Port that can receive and transmit I-tagged frames for multiple customers. PIPs are applicable only on PBB I Components.

Syntax **port-type providerInstancePort**

Mode `Interface Configuration Mode (Physical/ Portchannel)`

Note: This command executes only if

- PBB functionality is started in the bridge.
- Bridge Mode is Provider backbone bridge I-Component mode

Example

```
Your Product(config-if)# port-type providerInstancePort
```

Related Command(s)

- `no shutdown provider-backbone-bridge` - Initializes the PBB feature in the bridge.
- `set gmrp disable` – Globally disables GMRP feature on all ports of a switch.
- `set gvrp disable` – Globally disables GVRP feature on all ports of a switch.
- `shutdown garp` - Shuts down the GARP module in the switch on all ports and releases all memories used for the GARP module.
- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `no ethernet cfm start` – Shuts down an Ethernet CFM processing on the switch.
- `bridge-mode` - Sets the bridge mode of the Switch Provider as Backbone Bridge I component Mode.

sleep

Command Objective This command makes the SMIS to sleep for the given time. Sleep delays the SMIS CLI thread for the configured seconds. This value ranges between 1 and 65535in seconds.

Syntax **sleep <seconds(1-65535)>**

Mode Privileged EXEC Mode

Example

```
Your Product# sleep 51
```

rate-limit pause

Command Objective This command enables the pause ingress rate limit above which PAUSE frames are transmitted on the interface.

The no form of the command disables pause ingress rate limiting on a port.

Syntax **rate-limit pause [<high-watermark>] [<low-watermark>]**

no rate-limit pause

Parameter Description

- `<high-watermark>` - Configures the ingress rate equal to or above which PAUSE frames are transmitted. This value ranges between 1 and 80000000 kbps
- `<low-watermark>` - Configures the ingress rate below which transmission of PAUSE frames are stopped. This value ranges between 1 and 80000000 kbps.

Note: This parameter is not supported in all SMIS models.

Mode Interface Configuration Mode (Physical)

Example

```
Your Product (config-if)# rate-limit pause 400000 300000
```

cpu controlled learning

Command Objective This command enables software learning of MAC Address from the packets arriving on the interface instead of hardware learning of MAC address.

The no form of the command disables CPU controlled learning of MAC Address on the interface.

Syntax **cpu controlled learning**

no cpu controlled learning

Mode Interface Configuration Mode (Physical)

Example

```
Your Product (config-if)# cpu controlled learning
```

traffic-separation control

Command Objective This command configures the method for receiving control packets to CPU. This control ensures that the CPU processing capacity is utilized appropriately, according to the need of the protocol.

Syntax **traffic-separation control {system_default | user_defined |none}**

Parameter Description

- `System_default` - Configures the method for receiving control packets to CPU as system default.

This implies that the software can automatically install the ACL and QoS rules for all the control packets.

Note: If the configuration is changed from 'system_default' to 'user_defined' option, then all the default ACL/QoS rules for carrying protocol control packets to CPU are removed. Then user has to install the specific ACL/QoS rules, to carry the intended control packets to CPU for the processing.

- `User_defined` - Configures the method for receiving control packets to CPU as user defined. This implies that the software cannot automatically install the ACL and QoS rules for all the control packets. Only the administrator can install the required rules for receiving control packets to CPU

  Note: If the configuration is changed from 'user-defined' to system-default or none, all the default ACL filters are installed. Already existing (if any) user configured ACL rules in the system are not removed.

- `none` - Configures the method for receiving control packets to CPU as none.

  Note: If the configuration is changed from 'none' to 'system_default' option, then all the default ACL filters for carrying protocol control packets to CPU are removed and new set of filters will be installed. Each filter will be associated with Qos rules.

  If the configuration is changed from 'none' to 'user_defined' option, then all the default ACL filters for carrying protocol control packets to CPU are removed. Then user has to install the specific ACL/QoS rules, to carry the intended control packets to CPU for the processing.

Mode Global Configuration Mode

Default none

Example

```
Your Product (config)# traffic-separation control system_default
```

Related Command(s) `show access-lists` - Shows the configuration details.

mdix auto

Command Objective This command enables the MDI/MDIX Auto Crossover of the interface. The no form of the command disables the MDI/MDIX Auto Crossover of the interface and set the port as MDIX port.

Syntax **mdix auto**

no mdix auto

Mode Interface Configuration Mode

Default AutoCross is disabled

Example

```
Your Product(config-if)# mdix auto
```

Related Command(s) `set port` - Sets the port to MDI or MDIX mode

set port

Command Objective This command sets the port to MDI or MDIX mode. This command is hardware specific and mdix is the vice versa of mdi.

Syntax **set port { mdi | mdix }**

Parameter Description

- `mdi` - Sets the port to mdi mode. This is hardware specific where transmit pair are pins 1, 2 and the receive pair are 3,6 pins respectively for the particular port.
- `mdix` - Sets the port to mdix mode. This is hardware specific where transmit pair are pins 3, 6 and the receive pair are 1, 2 pins respectively for the particular port. mdix is the vice versa of mdi

Mode Interface Configuration Mode

Note: This command executes only when Auto cross is disabled.

Example

```
Your Product(config-if)# set port mdix
```

Related Command(s) `mdix port` - Enables the MDI/MDIX Auto Cross over of the interface

config-restore

Command Objective This command configures the startup configuration restore option. This feature is not available in some SMIS models.

Syntax **config-restore {flash | remote ip-addr <ip-address> file <filename> | norestore}**

Parameter Description

- `flash` - Restores the flash file that is to be used for restoration when the system is restarted
- `remote ip-addr <ip-address>` - Restores the IP address of the remote system from where the switch configurations have to be downloaded to the 'Startup Configuration File' in the flash.
- `file <filename>` - This restores the specified remote location file that is to be used for restoration. This is a string with maximum size as 12.
- `norestore` - Specifies that the switch configurations need not be restored when the system is restarted.

Mode Privileged EXEC Mode

Default norestore

Example Your Product# config-restore flash

Related Command(s) `show system information` – Displays the system information.

set switch-name

Command Objective This command sets the name of the switch. This is a string with maximum size as 15.

Syntax **set switch-name <switchname>**

Mode Global Configuration mode

Example `Your Product(config)# set switch-name sw1`

Related Command(s) `show system information` – Displays the system information

packet receive index

Command Objective This command configures the packet pattern and mask for pattern matching on the received packets.

Syntax **packet receive index <integer (0-4)> {value | mask | port<port_list>}**
no packet receive index <integer(0-4)> [mask]

Parameter Description

- `<integer (0-4)>`-Configures the packet receive index value which uniquely identifies a pattern to be matched. This value ranges between 0 and 4.
- `value` - Sets a value for the pattern to match with the received packets.
- `mask` - Sets a value to mask the received packets. This value is the mask for the pattern to be matched by the packet analyser. This value ranges between 1 and 1600.
- `port <port_list>` - Configures the port / list of ports of the receiver pattern. This is the complete set of ports over which the pattern is to be matched by the packet. This value ranges between 1 and 320. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.

Mode Global Configuration Mode

Example `Your Product(config)# packet receive index 0 port 223`

Related Command(s) `show packet receive` - Displays the match ports and the timers of the Pattern Analyser.

packet send index port

Command Objective This command sets the port, interval, and count for the packet transmitter and transmits the packet provided the packet pattern is configured.

The no form of the command disables the packet transmitter for given index

Syntax **packet send index <integer (0-4)> port <port_list> [count <integer (0-65536)> [interval <integer (1-65535)>]]no packet send index <integer(0-4)>**

Parameter Description

- `<integer (0-4)>` -Configures the packet send index value which uniquely identifies a packet to be sent. This value ranges between 0 and 4.
- `port <port_list>` - Configures the port or port list of the receiver pattern. This value ranges between 1 and 320. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
- `count <integer (0-65536)>` - Configures the number of packet to be sent over the ports. This value ranges between 0 and 65536.
- `interval <integer (1-65535)>` - Configures the time interval for sending the packet over the port in seconds. This value ranges between 1 and 65535.

Mode Global Configuration Mode

Example

```
Your Product(config)# packet send index 1 port 5
```

Related Command(s) `show packet send index` - Displays the values of the packet transmitter table.

packet send index value

Command Objective This command sets the packet pattern for the packet transmitter and transmits the packet, provided the interface is configured. The packet send index ranges between 0 and 4 and the packet send value ranges between 1 and 1600.

The no form of the command disables the packet transmitter for given index.

Syntax **packet send index <integer (0-4)>**
value no packet send index <integer(0-4)>

Mode Global Configuration Mode

Example

```
Your Product(config)# packet send index 1 value
Enter Value: 4
```

Related Command(s) `show packet send index` - Displays the values of the packet transmitter table.

show packet send index

Command Objective This command displays the values of the packet transmitter table. The packet send index ranges between 0 and 4.

Syntax **show packet send index <integer(0-4)>**

Mode Privileged EXEC Mode

Example

```
Your Product# show packet send index 1
Index              : 1
Value of the Pkt   :
```

Related Command(s)

- `packet send index value`- Sets the port, interval, count for the packet transmitter and transmits the packet provided the packet pattern is configured.
- `packet send index port` - Sets the packet pattern for the packet transmitter and transmits the packet, provided the interface is configured.

show packet receive index

Command Objective This command displays the values of the packet receiver table. The packet receive index ranges between 0 and 4.

Syntax **show packet receive index <integer(0-4)>**

Mode Privileged EXEC Mode

Example

```
Your Product# show packet receive index 1
Packet Analyzer
```

Related Command(s) `packet receive index`- Configures the packet pattern and mask for pattern matching on the received packets.

set mirroring

Command Objective This command enables or disables the mirroring in the system

Syntax **set mirroring {enable | disable}**

Parameter Description

- `enable` – Enables mirroring in the system. When set as enabled all mirroring configurations present will be programmed in hardware.
- `disable`– Disables mirroring in the system and removes all configuration from the hardware

Mode Global Configuration Mode

Default enable

Example

```
Your Product(config)# set mirroring enable
```

Related Command(s) `show monitor all` - Displays the mirroring information present in the system.

default exec-timeout

Command Objective This command configures the default exec-timeout value for line disconnection. This value ranges between 1 and 18000 seconds.

Syntax **default exec-timeout <integer (1-18000)>**

no default exec-timeout

Mode Global Configuration Mode

Example

```
Your Product(config)# default exec-timeout 5
```

ip unnumbered

Command Objective This command configures the associated source interface for the unnumbered interface. This enables to communicate over unnumbered interface with the peer using source address as any one of the associated IP address configured to other interfaces.

The no form of the command removes associated source interface for the unnumbered interface.

Syntax **ip unnumbered ([<peer-mac>] [{[vlan <vlan-id/vfi-id>] | [<iftype> <ifnum>] | [loopback <loopback-id(0-100)>]}])**

no ip unnumbered ([<peer-mac>] [{[vlan <vlan-id/vfi-id>] | [<iftype> <ifnum>] | [loopback <loopback-id(0-100)>]}])

Parameter Description

- `<peer-mac>` - Configures the unicast peer mac address for unnumbered interface. This needs to be configured for proper forwarding of IP packets over unnumbered interfaces.
- `vlan <vlan-id/vfi-id>` - Configures the unnumbered interface for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - `<vfi-id>`. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

    Notes:

    1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
    2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
    3. The theoretical maximum for the maximum number of VFI is 65535 but the actual

number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- `<iftype>` - Configures the associated source address for the specified type of interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<ifnum>` - Configures the associated source interface for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.
- `loopback <loopback-id(0-100)>` - Configures the associated source address for the specified loopback. This value ranges between 0 and 100

Mode Interface Configuration Mode (VLAN)

Note: The interface should be shutdown before executing this command.

Example

```
Unnumbered interface for VLAN
Your Product(config)# int vlan 1
Your Product(config-if)# ip address 14.0.0.1 255.0.0.0
Your Product(config)# int vlan 2
Your Product(config-if)# ip unnumbered vlan 1
Unnumbered interface for unicast peer mac address
Your Product(config)# int vlan 1
Your Product(config-if)# ip address 14.0.0.1 255.0.0.0
Your Product(config)# int vlan 2
Your Product(config-if)# ip unnumbered 00:01:02:03:04:02
```

Related Command(s) `ip address` - Configures IP address for an interface.

clear http server statistics

Command Objective This command clears the HTTP server requests received and discarded statistics.

Syntax **clear http server statistics**

Mode Global Configuration Mode

Example

```
Your Product(config)# clear http server statistics
```

show license

Command Objective This command shows the license status for particular switch models. When the switch is not licensed and is locked in User EXEC Mode, this command will show the license application data on the screen, and users can copy the output of this command to send to technical support for licensing.

Syntax **show license**

Mode User EXEC Mode

Example

```
Your Product> show license
Hardware Version                  : P6-01
Switch Serial Number              : SSG36BR06B99988
Switch MAC Address                : 00-25-90-FF-FF-FF
Hardware Part Number              : SSE-G3648BR
License                           : Absent

Fingerprint                       :
{2bpfav0cGQyxDQavEQ4ADxYZGQsSDAEKGAQQGhYZGQwBChAaCAoQCAgIGAcWCAgSBxQSEwgSEA
cSAxgSChQWBRsEAQUCFAUSGBMKARIJCQsKEhADAhgSCAQICAcICBsTBQoKmfPGxPjBpPLw8fbFx
4WDlsKJYPn1lGqX9OLZww==}
```

install license

Command Objective This command installs a license file or license code to activate the switch. Only applicable to particular models.

Syntax **install license {tftp://ip-address/filename | usb:filename**

Mode User EXEC Mode

Example

```
Your Product> install license code
16586b36b83ecb81bf03e4ea5eb8619dea80302acf2d22f958a131aa9adc63f30e267c9a7e1
4a25ae79f12c916cc31bb459be7431e912135e7dce40c3f9539dd0946757c981b531379445c
2b7248d81abff4b696f16f86e32257a4ceeff83f7e3d2c4a218732976c360aba35af2c8bbee
05f2cd67e43d438e35bc77adae0b42bee63583a8e483c6f4005f9ddc0c1fad814ba73cf1628
18cbdad9f822f6bbfb588620115a52978125c3819e8419a96867ca019c429bf12a5c4bf3e31
b977e445d4e9a4e8f3ea61e05b2852f6a1df6b2c780c6fb0d15724536c035c2451e9c8350f1
f6b535fff3941e5981732355330483ffa0b63a21e630024d3b4d1ed064a98e
License code validated, activation procedure completed.
Operation successfully completed.
Rebooting the system...
Your Product> install license usb:my_license.lic
License code validated, activation procedure completed.
```

```
Operation successfully completed.
Rebooting the system...
Your Product> install license tftp://192.168.100.200/my_license.lic
License code validated, activation procedure completed.
Operation successfully completed.
Rebooting the system...
```

uninstall license

Command Objective This command deactivates the switch by removing the license. Only applicable to particular models.

Syntax **uninstall license**

Mode Global Configuration Mode

Example

```
Your Product(config)# uninstall license
This command will delete the license and reboot
the system, do you really want to proceed? [y/n]
License data cleared, rebooting the system...
```

copy debug-files

Command Objective Copy debug info files to a remote site or usb storage.

Syntax **copy debug-files {tftp://ip-address/filename | sftp://<user-name>:<pass-word>@ip-address/filename | usb:filename}**

Parameter Description

- `tftp://ip-address/filename` - Configures the TFTP details for taking back up of system logs in TFTP server.
  - `ip-address` - the IP address or host name of the TFTP server.
  - `filename` - The name of the file in which the system logs should be stored. Filenames and directory names are case sensitive
- `sftp://<user-name>:<pass-word>@ip-address/filename` - Configures the SFTP details for taking back up of system logs in SFTP server.
  - `user-name` - The user name of remote host or server.
  - `pass-word` **–** The password for the corresponding user name of remote host or server.
  - `ip-address` - The IP address or host name of the server.
  - `filename` - The name of the file in which the system logs should be stored. Filenames and directory names are case sensitive

Mode All Modes

Example `Your Product# copy debug-files tftp://10.0.0.10/test`

reset-to-factory-default

Command Objective Reset the switch to factory default and reboot the switch

Syntax **reset-to-factory-default [switch <switch-id> | all]**

Parameter Description

- `switch-id` - Select the switch unit number, only valid for stacking software
- `all` – Select all the stacking switch units, only valid for stacking software

Mode Global Configuration Mode

Example

```
Your Product(config)# reset-to-factory-default
```

ztp

Command Objective Enable or disable the ZTP (Zero Touch Provision) function, default is disabled

Syntax **ztp {enable | disable}**

Parameter Description

- `enable` - Enable ZTP, need reboot to take effect
- `disable` – Disable ZTP, need reboot to take effect if configuration has been loaded into the switch

Mode Global Configuration Mode

Example

```
Your Product(config)# ztp enable
```

onie bootmode

Command Objective Select ONIE boot mode to enter for next reload only. By the default, switch will boot to NOS.

Syntax **onie bootmode [{ install | uninstall | rescue | update | embed}]**

Parameter Description

- `install` - Enter ONIE install mode after switch reload
- `uninstall` – Enter ONIE uninstall mode after switch reload
- `rescue` – Enter ONIE rescue mode after switch reload
- `update` – Enter ONIE update mode after switch reload
- `embed` – Enter ONIE embed mode after switch reload

Mode Global Configuration Mode

Example

```
Your Product(config)# onie bootmode install
```

show transceiver

Command Objective display transceiver of the plugged interface, if the transceiver provides digital diagnostics monitoring (DDM) information, it will be displayed.

Syntax **show transceiver [<iftype> <ifnum>]**

Parameter Description

- `iftype` – Interface type
- `ifnum` – Interface number

Mode Privileged EXEC Mode

Example

```
Your Product# show transceiver
```

5 RADIUS

RADIUS (Remote Authentication Dial-In User Service), widely used in network environments, is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for embedded network devices such as routers, modem servers, switches and so on. RADIUS is currently the de-facto standard for remote authentication. It is very prevalent in both new and legacy systems. It is used for several reasons:

- RADIUS facilitates centralized user administration (Authentication, Authorization and Accounting).
- RADIUS consistently provides some level of protection against an active attacker.

The list of CLI commands for the configuration of RADIUS is as follows:

- radius-server host
- debug radius
- show radius server
- show radius statistics

Note: The privilege level though RADIUS is not supported.

radius-server host

Command Objective This command configures the RADIUS client with the parameters (host, timeout, key, retransmit).

The no form of the command deletes RADIUS server configuration.

Syntax **radius-server host {ipv4-address | ipv6-address | host- name} [auth-port <integer(1-65535)>] [acct-port <integer(1-65535)>] [timeout <1-120>] [retransmit <1-254>][key <secret-key-string>] [primary]**

no radius-server host {ipv4-address | ipv6-address | host- name} [primary]

Parameter Description

- `ipv4-address` - Configures the IPv4 address of the RADIUS server host.
- `ipv6-address` - Configures the IPv6 address of the RADIUS server host.
- `host-name` - Configures the DNS (Domain Name System) name of the RADIUS server host. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
- `auth-port <integer(1-65535)>` - Configures a specific UDP (User Datagram Protocol) destination port on this RADIUS server to be used solely for the authentication requests. The value of the auth port ranges between 1 and 65535.
- `acct-port <integer(1-65535)>` - Configures a specific UDP destination port on this RADIUS to be solely used for accounting requests. The value of the auth port ranges between 1 and 65535.
- `timeout <1-120>` - Configures the time period in seconds for which a client waits for a response from the server before re-transmitting the request. The value of the time out in ranges between 1 to 120 in seconds.
- `retransmit <1-254>` - Configures the maximum number of attempts the client undertakes to contact the server. The value number of retransmit attempts ranges between 1 and 254
- `key <secret-key-string>` - Configures the Per-server encryption key which specifies the authentication and encryption key for all RADIUS communications between the authenticator and the RADIUS server. The value of the maximum length of the secret key string is 46.
- `primary` - Sets the RADIUS server as the primary server. Only one server can be configured as the primary server, any existing primary server will be replaced, when the command is executed with this option.

Mode Global Configuration Mode

Default

- `timeout` - 10 seconds
- `retransmit` - 3 attempts
- `key` - empty string

Example Your Product (config)# radius-server host 10.0.0.1 key pass

Related Command(s)

- `aaa authentication dot1x default` - Enables the dot1x local authentication or RADIUS server based remote authentication method for all ports

- `show radius server` - Displays RADIUS server configuration
- `show radius statistics` - Displays RADIUS statistics

debug radius

Command Objective This command enables RADIUS debugging options. The radius debug traces capture error information and failure messages in the server. These are registered in a log file for future reference. Each trace has to be enabled individually.

The no form of the command disables RADIUS debugging options.

Syntax **debug radius {all | errors | events | packets | responses | timers}**

no debug radius

Parameter Description

- `all` - Generates traces for all the RADIUS server messages
- `errors` - Generates traces for error code messages. All the instances where an error is identified are captured by this trace. The error is registered in the log.
- `events` - Generates traces for events related messages. Events like authentication query from authenticator, response from server are registered in the log.
- `packets` - Generates traces for number of packets, kind of packets received and sent from server.
- `responses` - Generates traces for responses sent from the server to authenticator.
- `timers` - Generates traces for the different timers used in the session before the system is reboot.

Mode Privileged EXEC Mode

Default Debugging is Disabled

Example

```
Your Product# debug radius all
```

show radius server

Command Objective This command displays RADIUS server Host information which contains, Index, Server address, Shared secret, Radius Server status, Response Time, Maximum Retransmission, Authentication Port and Accounting Port.

Syntax **show radius server [{<ucast_addr> | <ip6_addr> | <string>}]**

Parameter Description

- `<ucast_addr>` - Displays the related information of the specified unicast address of the RADIUS server host.
- `<ip6_addr>` - Displays the related information of the specified IPv6 address of the RADIUS server host.

- `<string>` - Displays the name of the RADIUS server host. This maximum value of the string is of size 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show radius server
Primary Server           : 2005::33
Radius Server Host Information
--------------------------------------------- Index                    : 1
Server address           : 13.0.0.100
Shared secret            : SupermicroRADIUS Radius Server Status     : Enabled
Response Time            : 10
Maximum Retransmission   : 3
Authentication Port      : 1812
Accounting Port          : 1813
------------------------------------------------------------------ Index                    : 2
Server address           : 2005::33
Shared secret            : SupermicroRADIUS Radius Server Status     : Enabled
Response Time            : 10
Maximum Retransmission   : 3
Authentication Port      : 1812
Accounting Port          : 1813
```

Related Command(s) `radius-server host` - Configures the RADIUS client with the parameters

show radius statistics

Command Objective This command displays RADIUS Server Statistics for the data transfer between server and the client from the time of initiation.

Syntax **show radius statistics**

Mode Privileged EXEC Mode

Example

```
Your Product# show radius statistics
Radius Server Statistics
---------------------------------------
Index               : 1
Radius Server Address                    : 10.0.0.1
UDP port number                   : 1812
Round trip time                   : 0
No of request packets                    : 8
No of retransmitted packets       : 80
No of access-accept packets    : 0 No
of access-reject packets    : 0 No of
access-challenge  packets  :  0  No  of
malformed access responses :  0
No of bad authenticators                 : 0
No of pending requests                   : 97
No of time outs                   : 89
No of unknown types               : 0
```

Related Command(s) `radius-server host` - Configures the RADIUS client with the parameters

6 TACACS

TACACS (Terminal Access Controller Access Control System), widely used in network environments, is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. It is commonly used for providing NAS (Network Access Security). NAS ensures secure access from remotely connected users. TACACS implements the TACACS Client and provides the AAA (Authentication, Authorization and Accounting) functionalities.

TACACS is used for several reasons:

- Facilitates centralized user administration.
- Uses TCP for transport to ensure reliable delivery.
- Supports inbound authentication, outbound authentication and change password request for the Authentication service.
- Provides some level of protection against an active attacker.

The list of CLI commands for the configuration of TACACS is as follows:

- tacacs-server host
- tacacs use-server address
- tacacs-server retransmit
- debug tacacs
- show tacacs

tacacs-server host

Command Objective This command configures the TACACS server with the parameters (host, timeout, key) and specifies the IP address of one or more TACACS and it specifies the names of the IP host or hosts maintaining a TACACS+ server.

The no form of the command deletes server entry from the TACACS server table.

Syntax **tacacs-server host {<ipv4-address> | <ipv6-address> | <host-name>} [single-connection] [port <tcp port (1-65535)>] [timeout <time out in seconds(1-255)>] {key <secret key>}**

no tacacs-server host { <ipv4-address> | <ipv6-address>}

Parameter Description

- <ipv4-address> - Configures the IPv4 address of the host
- <ipv6-address> - Configures the IPv6 address of the host
- <host-name> - Configures the DNS (Domain Name System) name of the TACACS server host. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
- single-connection - Allows multiple sessions to be established over a single TCP connection for AAA functionalities
- port<tcp port (1-65535)> - Configures the TCP port number in which the multiple sessions are established. The value ranges between 1 and 65535.
- timeout<time out in seconds(1-255)> - Configures the time period (in seconds) till which a client waits for a response from the server before closing the TCP connection. The link between the server and the client gets disconnected, if the specified time is exceeded. The value ranges from 1 to 255 seconds.
- key<secret key> - Specifies the authentication and encryption key for all TACACS communications between the authenticator and the TACACS server. The value is string of maximum length 64.

Mode Global Configuration Mode

Default

- port - 40
- timeout - 5 seconds

Example

```
Your Product (config)# tacacs-server host 12.0.0.100
TACACS+ server configured with default secret key !
Your Product (config)# tacacs-server host 2005::33
TACACS+ server configured with default secret key !
```

Related Command(s)

- show tacacs - Displays the server (such as IP address, Single connection, Port and so on) and statistical log information (such as Authen. Starts sent, Authen. Continues sent, Authen. Enables sent, Authen. Aborts sent and so on) for TACACS+ client.
- tacacs use-server address – Selects the server for the user from the list of configured servers.

tacacs use-server address

Command Objective This command configures the server IP address and an active server from the list of servers available in the TACACS server table.

The no form of the command disables the configured client active server.

Syntax **tacacs use-server address { <ipv4-address> | <ipv6- address>}**

no tacacs use-server

Parameter Description

- `<ipv4-address>` - Configures the IPv4 address of the host
- `<ipv6-address>` - Configures the IPv6 address of the host

Mode Global Configuration Mode

Note: The specified ip address should be any one of the entries from the TACACS server table

Example

```
Your Product (config)# tacacs use-server address 10.0.0.100
```

Related Command(s)

- `show tacacs` - Displays the server (such as IP address, Single connection, Port and so on) and statistical log information (such as Authen. Starts sent, Authen. Continues sent, Authen. Enables sent, Authen. Aborts sent and so on) for TACACS+ client.
- `tacacs-server host` – Creates the TACACS server entry in a TACACS server table
- `tacacs-server retransmit` - Configures the retransmit value which is the time interval (in seconds) till which the client waits for a response from active server.

tacacs-server retransmit

Command Objective This command configures the retransmit value. It is the number of times the client searches the active server from the list of servers maintained in the TACACS client, when active server is not configured. The retransmit value ranges from 1 to 100.

The no form of the command resets the retransmit value to its default value

Syntax **tacacs-server retransmit <retries>**

no tacacs-server retransmit

Mode Global Configuration Mode

Default 2

Example Your Product (config)# tacacs-server retransmit 3

Related Command(s) `tacacs use-server address` – Selects an active server from the list of servers available in the TACACS server table.

debug tacacs

Command Objective This command sets the debug trace level for TACACS client module. The no form of the command disables the debug trace level for TACACS client module.

Syntax **debug tacacs { all | info | errors | dumptx | dumprx }**

no debug tacacs

Parameter Description

- `all` - Generates debug messages for all possible traces (Dumptx, Dumprx, Error, Info).
- `info` - Generates debug statements for server information messages such as TACACS session timed out, server unreachability, Session ID exceeded and so on.
- `errors` - Generates debug statements for error debug messages such as failure caused during packet transmission and reception.
- `dumptx` - Generates debug statements for handling traces. This trace is generated when there is an error condition in transmission of packets.
- `dumprx` - Generates debug statements for handling traces. This trace is generated when there is an error condition in reception of packets.

Mode Privileged EXEC Mode

Default Debugging is Disabled

Example Your Product# debug tacacs all

show tacacs

Command Objective This command displays the server (such as IP address, Single connection, Port and so on) and statistical log information (such as Authen. Starts sent, Authen. Continues sent, Authen. Enables sent, Authen. Aborts sent and so on) for TACACS+ client.

Syntax show tacacs

Mode Privileged EXEC Mode

Note: It displays the information only for the servers configured in the TACACS server table.

Example

```
Your Product# show tacacs
Server : 1
Server address              : 12.0.0.100
Address Type                : IPV4
       Single Connection    : no
       TCP port             : 49
       Timeout              : 5
       Secret Key           : Supermicro
Server                      : 2
Server address              : 2005::33
Address Type                : IPV6
       Single Connection    : no
       TCP port             : 4949
       Timeout              : 5
       Secret Key           : Supermicro
```

```
Authen. Starts sent        : 0
Authen. Continues sent     : 0
Authen. Enables sent       : 0
Authen. Aborts sent        : 0
Authen. Pass rvcd.         : 0
Authen. Fails rcvd.        : 0
Authen. Get User rcvd.     : 0
Authen. Get Pass rcvd.     : 0
Authen. Get Data rcvd.     : 0
Authen.   Errors rcvd.     : 0
Authen.   Follows rcvd.    : 0
Authen.   Restart rcvd.    : 0
Authen.   Sess. Timeouts   : 0
Author.   Requests sent    : 0
Author.   Pass Add rcvd.   : 0
Author.   Pass Repl rcvd   : 0
Author.   Fails rcvd.      : 0
Author.   Errors rcvd.     : 0
Author Follows rcvd.       : 0
Author. Sess. Timeouts     : 0
Acct. start reqs. Sent     : 0
Acct. WD reqs. Sent        : 0
Acct. Stop reqs. Sent      : 0
Acct. Success rcvd.        : 0
Acct. Errors rcvd.         : 0
Acct. Follows rcvd.        : 0
Acct. Sess. Timeouts       : 0
Malformed Pkts. rcvd.      : 0
Socket failures            : 0
Connection failures        : 0
```

Related Command(s)

- `tacacs-server host` - Creates a TACACS server entry in a TACACS server
- `tacacs use-server address` - Configures an active server from the list of servers available in the TACACS server table

7 SSH

SSH (Secure Shell) is a protocol for secure remote login and other secure network services over an insecure network. It consists of three major components:

- The Transport Layer Protocol provides server authentication, confidentiality and integrity.
- The User Authentication Protocol authenticates the client-side user to the server. It runs over the transport layer protocol.
- The Connection Protocol multiplexes the encrypted tunnel into several logical channels. It runs over the user authentication protocol.

The client sends a service request once a secure transport layer connection has been established. A second service request is sent after user authentication is complete. This allows new protocols to be defined and coexist with these protocols.

The list of CLI commands for the configuration of SSH is as follows:

- ip ssh
- ssh
- debug ssh
- show ip ssh
- ip ssh transport-max-allowed bytes
- ip ssh pubkey-chain
- ssh server-address
- show ssh-configurations

ip ssh

Command Objective This command configures the various parameters associated with SSH server. The standard port used by SSH is 22. SSH server allows remote and secure configuration of the switch. The SSH server provides protocol version exchange, data integrity, cipher and key exchange algorithms negotiation between two communicating entities, key exchange mechanism, encryption and server authentication. The auth takes values as bit mask. Setting a bit indicates that the corresponding MAC-list will be used for authentication. The no form of this command re-sets the various parameters associated with SSH server.

Syntax **ip ssh {version compatibility | cipher ([des-cbc] [3des- cbc] [aes128-cbc] [aes256-cbc]) | auth ([hmac-md5] [hmac- sha1]) }**

no ip ssh {version compatibility | cipher ([des-cbc] [3des- cbc] [aes128-cbc] [aes256-cbc]) | auth ([hmac-md5] [hmac- sha1]) }

Parameter Description

- `version compatibility` - Configures the version of the SSH. When set to true, it supports both SSH version-1 and version-2. When set to false, it supports only the SSH version-2.
- `cipher` - Configures the Cipher-List. This cipherlist takes values as bit mask. Setting a bit indicates that the corresponding cipher-list is used for encryption.
  - `des-cbc` **–**This is a 1 bit cipherlist. It is based on a symmetric-key algorithm that uses a 56-bit key.
  - `3des-cbc` **–** This is a 0 bit cipherlist. Triple DES provides a relatively simple method of increasing the key size of DES to protect against brute force attacks, without requiring a completely new block cipher algorithm.
  - `aes128-cbc` **–** This is a 2-bit cipherlist. Advanced Encryption Standard (AES) is a specification for the encryption of electronic data for 128 bits
  - `aes256-cbc` - This is a 3-bit cipherlist Advanced Encryption Standard (AES) is a specification

for the encryption of electronic data for 256 bits

- auth - Configures Public key authentication for incoming SSH sessions.

Mode Global configuration Mode

Default

- version compatibility - False
- cipher - 3des-cbc
- auth - hmac-sha1

Example

```
Your Product (config)#ip ssh version compatibility
Your Product (config)# ip ssh cipher des-cbc
```

Related Command(s)

- `show ip ssh` - Displays SSH server information.
- `ip ssh`- Enables or disables the ssh subsystem.
- `ssh` - Enables or disables the ssh subsystem

ssh

Command Objective This command either enables or disables the ssh subsystem. When set to enable, the switch is accessible through ssh from a remote locations. Setting ssh to disable, removes the ssh access to the switch.

Syntax **ssh {enable | disable}**

Parameter Description

- `enable` - Enables the ssh subsystem.
- `disable` - Disables the ssh subsystem.

Mode Global configuration Mode

Default enable

Example `Your Product# ssh enable`

Related Command(s) `ip ssh` - Configures the various parameters associated with SSH server

debug ssh

Command Objective This command enables the trace levels for SSH. System errors such as memory allocation failures are notified using LOG messages and TRACE messages. Interface errors and protocol errors are notified using TRACE messages. Setting all the bits will enable all the trace levels and resetting them will disable all the trace levels The no form of this command re-sets the SSH trace levels.

Syntax **debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer] [server])**

no debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer] [server])

Parameter Description

- `all` - Generates debug statements for all traces.
- `shut` - Generates debug statements for shutdown traces. This trace is generated on successful shutting down of SSH related module and memory.
- `mgmt` - Generates debug statements for management plane functionality traces.
- `data` - Generates debug statements for data path
- `ctrl` - Generates debug statements for Control Plane functionality traces
- `dump` - Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.
- `resource` - Generates debug statements for traces with respect to allocation and freeing of all resource except the buffers.
- `buffer` - Generates debug statements for traces with respect to allocation and freeing of buffer.
- `server` - Generates debug statements while creating/ opening/ closing SSH server sockets and any failures to wake up SSH server sockets. Also generates debug statements during enabling /disabling of SSH server.

Mode Privileged EXEC Mode

Default Debugging is Disabled

Example `Your Product# debug ssh all`

Related Command(s) `show ip ssh` - Displays SSH server information

show ip ssh

Command Objective This command displays the SSH server information such as version, cipher algorithm, authentication and trace level.

Syntax **show ip ssh**

Mode Privileged EXEC Mode

Example

```
Your Product# show ip ssh
Version          : 2
Cipher Algorithm : 3DES-CBC Authentication      : HMAC-SHA1
Trace Level      : None
Max Byte Allowed :32768
```

Related Command(s)

- `ip ssh` - Enables SSH server on the device and configures the various parameters associated with SSH server
- `debug ssh` - Enables the trace levels for SSH.
- `ip ssh transport-max-allowed bytes` - configure the maximum number of bytes allowed in an SSH transport connection

ip ssh transport-max-allowed bytes

Command Objective This command configures the maximum number of bytes allowed in an SSH transport connection. The maximum allowed bytes ranges between 1 and 32768. The SSH connection will be allowed only if the packet size does not exceed the value configured and is dropped if the value exceeds the configured.

Syntax `ip ssh transport-max-allowed bytes <integer(1-32768)>`

Mode Global configuration Mode

Example `Your Product# ip ssh transport-max-allowed bytes 1`

Related Command(s) `show ip ssh` – Displays SSH server information

ip ssh pubkey-chain

Command Objective This command configures the SSH clients public key, to be used for public key based authentication.

The no form of the command disables the SSH clients public key that is to be used for public key based authentication.

Syntax **ip ssh pubkey-chain**

no ip ssh pubkey-chain

Mode Privileged EXEC Mode

Example `Your Product# ip ssh pubkey-chain`

Related Command(s) `show ip ssh` - Displays SSH server information

ssh server-address

Command Objective This command configures the SSH server listening IP address and the primary port number.

Syntax **ssh server-address <ip-address> [port <integer(1-65535)>]**

Parameter Description

- `server-address <ip-address>` - Configures the listening IP address on the SSH server.
- `port <integer(1-65535)>]` - Configures the primary port number on which SSH server listens. This value reanges between 1 and 65535.

Mode Global Configuration Mode

Default Port - 22

Example

```
Your Product (config)# ssh server-address 12.0.0.0 port 1
```

Related Command(s) `show ssh-configurations` - Displays the SSH server listening IP and port informations.

show ssh-configurations

Command Objective This command displays the SSH server listening IP address and port information.

Syntax **show ssh-configurations**

Mode Privileged EXEC Mode

Example

```
Your Product# show ssh-configurations
SSH Listening IP 12.0.0.0
Port 1
```

Related Command(s) `ssh server-address` - Configures the SSH server listening IP address and the primary port number.

8 SSL

SSL (Secure Sockets Layer), is a protocol developed for transmitting private documents through Internet. It works by using a private key to encrypt data that is transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:

The SSL Protocol is designed to provide privacy between two communicating applications (a client and a server) and is designed to authenticate the server, and optionally the client. SSL requires a reliable transport protocol (for example, TCP) for data transmission and reception.

The advantage of the SSL Protocol is that it is application protocol independent. A higher level application protocol (for example, HTTP, FTP, TELNET and so on.) can layer on top of the SSL Protocol transparently. The SSL Protocol can negotiate an encryption algorithm and session key as well as authenticate a server before the application protocol transmits or receives its first byte of data. All of the application protocol data is transmitted encrypted, ensuring privacy.

The list of CLI commands for the configuration of SSL is as follows:

- ip http secure
- ssl gen cert-req algo rsa sn
- ssl server-cert
- debug ssl
- show ssl server-cert
- show ip http secure server status
- version

ip http secure

Command Objective This command enables SSL server on the device and also configures ciphersuites and crypto keys.

The no form of the command disables SSL server on the device and also disables ciphersuites and crypto key configuration.

Syntax **ip http secure { server | ciphersuite [rsa-null-md5] [rsa- null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des-sha][dh-rsa-3des-sha][rsa-exp1024-des-sha] [rsa-with-aes-128-cbc-sha] [rsa-with-aes-256-cbc-sha] [dhe-rsa-with-aes-128- cbc-sha] [dhe-rsa-with-aes-256-cbc-sha] | crypto key rsa [usage-keys (512|1024)]}**

no ip http secure { server | ciphersuite [rsa-null-md5] [rsa-null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des- sha] [dh-rsa-3des-sha] [rsa-exp1024-des-sha] [rsa-with-aes-128-cbc-sha] [rsa-with-aes-256-cbc-sha] [dhe-rsa-with-aes-128-cbc-sha] [dhe-rsa-with-aes-256-cbc-sha]}

Parameter Description

- `server` - Configures the server status to be enabled. When the server status is enabled it establishes the secure layer in the network
- `ciphersuite` - Configures the ciphersuite for providing the input. When an SSL connection is established, the client and server exchange information about which cipher suites they have in common. The options are:
  - `rsa-null-md5` – cipher suites using RSA key exchange. and offering no authentication combined with cipher suites using MD5

- `rsa-null-sha` – cipher suites using RSA key exchange. and offering no authentication combined with cipher suites using SHA1 .
- `rsa-des-sha` – cipher suites using RSA key exchange. and cipher suites using DES, combined with cipher suites using SHA1
- `rsa-3des-sha` – cipher suites using RSA key exchange. and cipher suites using triple DES, combined with cipher suites using SHA1
- `dh-rsa-des-sha` – cipher suites using DH , including anonymous DH with cipher suites using RSA key exchange. and cipher suites using DES, combined with cipher suites using SHA1
- `dh-rsa-3des-sha` – cipher suites using DH , including anonymous DH with cipher suites using RSA key exchange. and cipher suites using triple DES, combined with cipher suites using SHA1
- `rsa-exp-1024-des-sha` – cipher suites using RSA key exchange with export encryption algorithms. Including 40 and 56 bits algorithms and cipher suites using DES, combined with cipher suites using SHA1
- `rsa-with-aes-128-cbc-sha` - cipher suites using RSA key exchange with a 2-bit cipherlist Advanced Encryption Standard (AES) algorithms and cipher suites using SHA1
- `rsa-with-aes-256-cbc-sha` - cipher suites using RSA key exchange with a 3-bit cipherlist Advanced Encryption Standard (AES) algorithms and cipher suites using SHA1
- `dhe-rsa-with-aes-128-cbc-sha` - cipher suites using dhe, and cipher suites using RSA key exchange with a 2-bit cipherlist Advanced Encryption Standard (AES) algorithms combined with cipher suites using SHA1
- `dhe-rsa-with-aes-256-cbc-sha` - cipher suites using dhe , and cipher suites using RSA key exchange with a 3-bit cipherlist Advanced Encryption Standard (AES) algorithms combined with cipher suites using SHA1

- `crypto key rsa[usage-keys (512|1024)]` - Configures the usage key (512 or 1024).

Mode Global Configuration Mode

Default ciphersuite - rsa-des-sha:rsa-3des-sha:rsa-exp1024-des-sha:

Example Your Product (config)# ip http secure ciphersuite rsa-null- sha

Related Command(s)

- `show ssl server-cert` - Displays SSL server certificate
- `show ip http secure server status` - Displays SSL status and configuration information

ssl gen cert-req algo rsa sn

Command Objective This command creates a request to generate a certificate to the certificate authority. This command uses the RSA key pair and subject name for generating the request. The subject name uniquely identifies the client by the certificate authority

Syntax **ssl gen cert-req algo rsa sn <SubjectName>**

Mode Privileged EXEC Mode

Example

```
Your Product# ssl gen cert-req algo rsa sn 10.6.4.248
```

Related Command(s)

- `show ssl server-cert` - Displays SSL server certificate.
- `show ip http secure server status` - Displays SSL status and configuration information

ssl server-cert

Command Objective This command configures the server-certificate input in PEM format. It imports the public certificate of the ssl server. When the ssl server certificate installation is complete, ssl server sends this certificate for authentication of client

Syntax **ssl server-cert**

Mode Privileged EXEC Mode

Note: The certificate request must have been created.

Example

```
Your Product# ssl server-cert
```

Related Command(s)

- `show ssl server-cert` - Displays SSL server certificate
- `show ip http secure server status` - Displays SSL status and configuration information

debug ssl

Command Objective This command configures the debug trace messages levels for SSL. System errors such as memory allocation failures are notified using LOG messages and TRACE messages. Interface errors and protocol errors are notified using TRACE messages.

The no form of the command re-sets the given SSL debug level.

Syntax **debug ssl ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer])**

no debug ssl ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer])

Parameter Description

- all - Generates debug statements for all traces.
- shut - Generates debug statements for shutdown traces. This trace is generated on successful shutting down of SSL related module and memory.
- mgmt - Generates debug statements for management plane functionality traces.

- data - Generates debug statements for datapath.
- ctrl - Generates debug statements for Control Plane functionality traces.
- dump - Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.
- resource - Generates debug statements for Traces with respect to allocation and freeing of all resource except the buffers.
- buffer - Generates debug statements for traces with respect to allocation and freeing of buffer.

Mode Privileged EXEC Mode

Default Disabled

Example Your Product# debug ssl all

Related Command(s)

- show ssl server-cert - Displays SSL server certificate
- show ip http secure server status - Displays SSL status and configuration information

show ssl server-cert

Command Objective This command displays SSL server certificate information such as Certificate, Data, version, serial number, Signature algorithm.

Syntax **show ssl server-cert**

Mode Privileged EXEC Mode

Note: SSL server certificate must have been created.

Example

```
Your Product# show ssl server-cert
Certificate:
Data:
       Version: 1 (0x0)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
Issuer: C=in, ST=tn, L=ch, O=fsoft,OU=ps,
CN=dheepaag/Email=products@Supermicro.com
       Validity
       Not Before: Jan 12 07:40:35 2005 GMT Not After : Feb 11 07:40:35
       2005 GMT Subject: CN=dee
       Subject Public Key Info:
       Public Key Algorithm:rsaEncryption
       RSA Public Key: (1024bit)
       Modulus (1024 bit):
       00:b1:cf:8f:04:39:c4:80:bc:f0:2b:40:e0:85:16:
       86:8f:cf:66:84:db:0d:fd:58:d5:fc:12:be:4d:d2:
       e2:ba:d6:d8:95:7c:9d:28:46:45:b3:8a:34:dd:41:
       c2:a3:46:ad:8f:c4:ae:17:37:22:91:c4:0a:8d:79:
```

```
      ce:10:34:2c:62:a5:6e:4c:a9:63:2e:93:46:a6:d2:
      1c:13:b7:38:02:fb:db:5f:13:46:8e:fb:df:7b:e7:
      c8:ba:00:ad:b2:96:cc:1c:4a:8b:2d:51:27:df:eb:
      9a:8f:6a:b2:8a:98:92:8e:6a:ed:ba:2e:04:38:3a:
      bf:40:f2:d1:37:6c:69:ed:d1
      Exponent:65537(0x10001) Signature Algorithm: md5WithRSAEncryption
8c:d2:50:01:5c:08:d1:0f:ef:eb:70:56:8e:ea:85:72:32:53:
13:0f:9c:7c:d6:d2:f6:2b:e4:6f:25:4e:86:08:5a:e2:c9:87:
65:cf:98:6c:99:86:a5:55:66:23:b5:b0:f4:56:e6:35:5e:53:
31:00:bc:9f:00:62:34:d1:15:c0:a4:7e:d9:27:c3:d2:d7:01:
13:18:ee:de:f8:52:c8:90:1c:8b:57:15:50:56:8c:b6:7b:4d:
77:e8:23:41:82:dc:9c:47:66:fb:9a:ba:7f:73:a1:d0:88:93:
7b:c3:4b:c8:a5:ec:db:4a:36:19:02:c9:f7:e6:d1:c7:38:d3:
13:f3
```

Related Command(s)

- `ip http secure` - Enables SSL server on the device and also configures ciphersuites and crypto keys
- `ssl gen cert-req algo rsa sn` - Creates a certificate request using RSA key pair and subjectName
- `ssl server-cert` - Configures the server cert, input in PEM format
- `show ip http secure server status` - Displays SSL status and configuration information

show ip http secure server status

Command Objective This command displays SSL status and configuration information. Information such as HTTP secure server status, http secure server ciphersuite are displayed.

Syntax **show ip http secure server status**

Mode Privileged EXEC Mode

Note: This command will display output only if http secure server ciphersuite and crypto keys are configured.

Example

```
Your Product# show ip http secure server status
HTTP secure server status      : Enabled
HTTP secure server ciphersuite : RSA-DES-SHA:RSA-3DES- SHA:RSA-EXP1024-DES-
SHA:
```

Related Command(s)

- `ip http secure` - Enables SSL server on the device and also configures ciphersuites and crypto keys
- `ssl gen cert-req algorsa sn` - Creates a certificate request using RSA key pair and subjectName
- `ssl server-cert` - Configures the server cert, input in PEM format

- `show ssl server-cert` - Displays SSL server certificate

version

Command Objective This command configures the SSL version.

Syntax **version {all | ssl3 | tls1}**

Parameter Description

- `all` - Allows configuration to both SSL3 and TLS1 SSL protocols. Server accepts all the connection and the https session is established.
- `ssl3` - Configures SSL version 3 protocol.
- `tls1` - Configures Transport Layer Security version 1 protocol.

Mode Global Configuration Mode

Default tls1

Example `Your Product(config)# version ssl3`

Related Command(s) `show ip http secure server status` - Displays SSL status and configuration information

9 SNTP

The SNTP (Simple Network Time Protocol) is a simplified version or subnet of the NTP protocol. It is used to synchronize the time and date in SMIS by contacting the SNTP Server. The administrator can choose whether to set the system clock manually or to enable SNTP. If SNTP is enabled, the SNTP implementation discovers the SNTP server and gets the time from the server. The SNTP implementation also has callouts to set the system time based on the time received from the SNTP server. It supports different time zones, where the user can set the required time zone.

The following are the list of SNTP commands:

- sntp
- set sntp client
- set sntp client version
- set sntp client addressing mode
- set sntp client port
- set sntp client clock-format
- set sntp client time zone
- set sntp client clock-summer-time
- set sntp client authentication-key

- set sntp unicast-server auto-discovery
- set sntp unicast-poll-interval
- set sntp unicast-max-poll-timeout
- set sntp unicast-max-poll-retry
- set sntp unicast-server
- set sntp broadcast-mode send-request
- set sntp broadcast-poll-timeout
- set sntp broadcast-delay-time
- set sntp multicast-mode send-request
- set sntp multicast-poll-timeout
- set sntp multicast-delay-time
- set sntp multicast-group-address
- set sntp manycast-poll-interval
- set sntp manycast-poll-timeout
- set sntp manycast-poll-retry-count
- set sntp manycast-server
- show sntp clock
- show sntp status
- show sntp unicast–mode status
- show sntp broadcast–mode status
- show sntp multicast–mode status
- show sntp manycast–mode status
- debug sntp
- show sntp statistics

sntp

Command Objective This command enters to SNTP configuration mode which allows the user to execute all the commands that supports SNTP configuration mode.

Syntax **sntp**

Mode Global Configuration Mode

Example

```
Your Product (config)# sntp
Your Product (config-sntp)#
```

Related Command(s)

- `set sntp client` – Sends the request to the host for time synchronization.
- `set sntp client version` - Sets the operating version of the client SNTP.
- `set sntp client addressing mode` - Sets the addressing mode of SNTP client.
- `set sntp client port`- Sets the listening port for SNTP client which refers to a port on a server that is waiting for a client connection.

- set sntp client clock format - Sets the system clock as either AM PM / HOURS format.
- set sntp client time zone - Sets the system time zone with respect to UTC.
- sntp client clock-summer-time- Enables the DST. (Daylight Saving Time).
- set sntp client authentication key - Sets the authentication key for the SNTO clients.
- set sntp unicast-server auto-discovery - Configures SNTP client status of auto-discovery
- set sntp unicast-poll-interval- Configures SNTP client poll interval.
- set sntp unicast-max-poll-timeout- Configures SNTP client maximum poll interval
- set sntp unicast-max-poll-retry - Configures SNTP client maximum retry poll count.
- set sntp unicast-server- Configures SNTP unicast server.
- set sntp broadcast-mode send request - Sets the status of sending the request for knowing the delay.
- set sntp broadcast-poll-timeout- Configures SNTP client poll interval in broadcast mode.
- set sntp broadcast-delay-time- Configures SNTP delay time in broadcast mode.
- set sntp multicast-mode send-request - Sets the status of sending the request for knowing the delay.
- set sntp multicast-poll-timeout - Configures SNTP client poll interval in multicast mode.
- set sntp multicast-delay-time - set sntp multicast-delay-time - Configures SNTP delay time in multicast mode.
- set sntp multicast-group-address- Configures SNTP multicast server address.
- set sntp manycost-poll-interval– Configures SNTP client poll interval in manycast mode.
- set sntp manycast-poll-timeout - Configures SNTP client poll timeout in manycast mode.
- set sntp manycast-poll-retry-count - Configures SNTP poll retries in manycast mode.
- set sntp manycast-server- Configures SNTP multicast or broadcast server address in manycast mode.

set sntp client

Command Objective This command either enables or disables SNTP client module.

Syntax **set sntp client {enabled | disabled}**

Parameter Description

- enabled - Enables SNTP client module and sends a request to the host for time synchronization.
- disabled - Disables SNTP client module and no request is sent to the host for time synchronization.

Mode SNTP Configuration Mode

Default Disabled

Example

```
Your Product (config-sntp)# set sntp client enabled
```

Related Command(s)

- sntp - Enters to SNTP configuration mode

- `show sntp status` - Displays the status of SNTP client.

set sntp client version

Command Objective This command sets the operating version of the SNTP for the client.

Syntax **set sntp client version { v1 | v2 | v3 | v4 }**

Parameter Description

- `v1` - Sets the version of SNTP client as 1
- `v2` - Sets the version of SNTP client as 2
- `v3` - Sets the version of SNTP client as 3
- `v4` - Sets the version of SNTP client as 4

Mode SNTP Configuration Mode

Default v4

Example

```
Your Product (config-sntp)# set sntp client version v3
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode.
- `show sntp status` - Displays the status of SNTP client.

set sntp client addressing mode

Command Objective This command sets the addressing mode of SNTP client.

Syntax

```
set sntp client addressing-mode {unicast | broadcast |multicast | manycast}
```

Parameter Description

- `unicast` - Sets the addressing mode of SNTP client as unicast which operates in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the round-trip delay and local clock offset relative to the server.
- `broadcast` - Sets the addressing mode of SNTP client as broadcast which operates in a point-to-multipoint fashion. The SNTP server uses an IP local broadcast address instead of a multicast address. The broadcast address is scoped to a single subnet, while a multicast address has Internet wide scope.
- `multicast` - Sets the addressing mode of SNTP client as multicast which operates in point-to-multipoint fashion. The SNTP server uses a multicast group address to send unsolicited SNTP messages to clients. The client listens on this address and sends no requests for updates.
- `manycast` - Sets the addressing mode of SNTP client as manycast which operates in a multipoint-to-point fashion. The SNTP client sends a request to a designated IPv4 or IPv6 local broadcast address

or multicast group address. One or more manycast servers reply with their individual unicast addresses.

Mode **SNTP Configuration Mode**

Default unicast

Example `Your Product (config-sntp)# set sntp client addressing- mode unicast`

Related Command(s)

- `sntp` - Enters to SNTP configuration mode.
- `show sntp status` - Displays SNTP status.
- `show sntp unicast-mode status` - Displays the SNTP unicast mode status.
- `show sntp broadcast-mode status` – Displays the SNTP broadcast mode status.
- `show sntp multicast-mode status` – Displays the SNTP multicast mode status.
- `show sntp manycast-mode status` – Displays the SNTP manycast mode status.

set sntp client port

Command Objective This command sets the listening port for SNTP client which refers to a port on a server that is waiting for a client connection. The value ranges between 1025 and 65535.

The no form of this command deletes the listening port for SNTP client and sets the default value.

Syntax **set sntp client port <portno(1025-65535)>**

no sntp client port

Mode **SNTP Configuration Mode**

Default **123**

Note: This command is executed only if SNTP client is enabled

Example `Your Product (config-sntp)# set sntp client port 1026`

Related Command(s)

- `sntp` - Enters to SNTP configuration mode.
- `show sntp status` - Displays SNTP status.

set sntp client clock-format

Command Objective This command sets the system clock as either AM PM format or HOURS format.

Syntax **set sntp client clock-format {ampm | hours}**

Parameter Description

- `ampm` - Sets the system clock in am/ pm format
- `hours` - Sets the system clock in 24 hours format

Mode SNTP Configuration Mode

Default hours

Example `Your Product (config-sntp)# set sntp client clock-format ampm`

Related Command(s)

- `sntp` - Enters to SNTP configuration mode.
- `show sntp status` - Displays SNTP status.
- `show sntp clock` - Displays the current time.

set sntp client time zone

Command Objective This command sets the system time zone with respect to UTC. The no form of command resets the system time zone to GMT.

Syntax **set sntp client time-zone <UTC-offset value as (+HH:MM /- HH:MM)(+00:00 to +14:00)/ (-00:00 to -12:00)> Eg: +05:30**

no sntp client time-zone

Parameter Description

- `+/-` - Sets the client time zone as after or before UTC. Plus indicates forward time zone and minus indicates backward time zone.
- `UTC-offset value as` - Sets the UTC offset value in hours
  - +00:00 to +14:00
  - -00:00 to -12:00

Mode SNTP Configuration Mode

Default + 00: 00

Example `Your Product (config-sntp)# set sntp client time-zone +05:30`

Related Command(s)

- `sntp` - Enters to SNTP configuration mode
- `show sntp status` - Displays SNTP status.

set sntp client clock-summer-time

Command Objective This command enables the DST (Daylight Saving Time). DST is a system of setting clocks ahead so that both sunrise and sunset occur at a later hour. The effect is additional daylight in the evening. Many countries observe DST, although most have their own rules and regulations for when it begins and ends. The dates of DST may change from year to year.

The no form of this command disables the Daylight Saving Time.

Syntax **set sntp client clock-summer-time <week-day-month,hh:mm> <week-day-month,hh:mm> Eg: set sntp client clock-summer- time First-Sun-Mar,05:10 Second-Sun-Nov,06:10**

no sntp client clock summer-time

Parameter Description

- `week-day-month` – The list is given below;
  - `week` **–** First, Second, Third, Fourth or Last week of month.
  - `day` **–**Sunday, Monday, Tuesday, Wednesday, Thursday, Friday or
  - `Saturday`.
  - `month`: January, February, March, April, May, June, July, August, September, October, November or December.
  - `hh:mm` - Time in hours and minutes

Mode SNTP Configuration Mode

Default Not set

Example

```
Your Product (config-sntp)# set sntp client clock-summer- time First-Sun-
Jan,12:12 Second-Sun-Mar,12:12
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode
- `show sntp status` - Displays SNTP status.

set sntp client authentication-key

Command Objective This command sets the authentication parameters for the key. Some SNTP severs requires authentication to be done before exchanging any data. This authentication key is used to authenticate the client to the SNTP server to which it tries to connect.

The no form of this command disables authentication.

Syntax **set sntp client authentication-key <key-id> {md5 | des} <key>**

no sntp client authentication

Parameter Description

- `<key-id>` - Sets a key identifier (integer value) to provide authentication for the server. The value ranges between 1 and 65535.
- `md5` - Sets authentication type as md5 where data is verified. MD5 is intended to use with digital signature applications, which requires large files are compressed by a secure method before being encrypted with a secret key, under a public key cryptosystem.
- `des` - Sets authentication type as data encryption standard algorithm.
- `<key>` - Sets the authentication code as a key value.

Mode SNTP Configuration Mode

Default Authentication key ID not set

Example

```
Your Product (config-sntp)# set sntp client authentication- key 123 md5
Aricent
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode
- `show sntp status` - Displays SNTP status.

set sntp unicast-server auto-discovery

Command Objective This command discovers the entire available SNTP client.

Syntax **set sntp unicast-server auto-discovery {enabled | disabled}**

Parameter Description

- **enabled** - Automatically discovers the entire available SNTP client even if the necessary configuration is not done.
- **disabled** - Does not discover any SNTP client.

Mode SNTP Configuration Mode

Default Disabled

Example

```
Your Product (config-sntp)# set sntp unicast-server auto- discovery enabled
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode.
- `Show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.

set sntp unicast-poll-interval

Command Objective This command sets the SNTP client poll interval which is the maximum interval between successive messages in seconds. The value ranges between 16 and 16284 seconds.

Syntax **set sntp unicast-poll-interval <value (16-16284) seconds>**

Mode SNTP Configuration Mode

Default 64

Example Your Product (config-sntp)# set sntp unicast-poll-interval 50

Related Command(s)

- `sntp` - Enters to SNTP configuration mode
- `show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.

set sntp unicast-max-poll-timeout

Command Objective This command configures SNTP client maximum poll interval timeout which is the maximum interval to wait for the poll to complete. The value ranges between 1 and 30 in seconds.

Syntax **set sntp unicast-max-poll-timeout <value (1-30) seconds>**

Mode SNTP Configuration Mode

Default 5

Example `Your Product (config-sntp)# set sntp unicast-max-poll- timeout 25`

Related Command(s)

- `sntp` - Enters to SNTP configuration mode.
- `show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.

set sntp unicast-max-poll-retry

Command Objective This command configures SNTP client maximum retry poll count which is the maximum number of unanswered polls that cause a slave to identify the server as dead. The value ranges between 1 and 10 in times.

Syntax **set sntp unicast-max-poll-retry <value (1-10) times>**

Mode SNTP Configuration Mode

Default 3

Example `Your Product (config-sntp)# set sntp unicast-max-poll- retry 10`

Related Command(s)

- `sntp` - Enters to SNTP configuration mode
- `show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.

set sntp unicast-server

Command Objective This command configures SNTP unicast server.

The no form of this command deletes the sntp unicast server attributes and sets to default value.

Syntax **set sntp unicast-server {ipv4 <ucast_addr> | ipv6 <ip6_addr> | domain-name <string(64)>} [{primary | secondary}] [version {3 | 4 }] [port <integer(1025-36564)>]**

no sntp unicast-server {ipv4 <ucast_addr> | ipv6 <ip6_addr> | domain-name <string(64)>}

Parameter Description

- `ipv4 <ucast_addr>` - Sets the address type of the unicast server as Internet Protocol Version 4.
- `ipv6 <ip6_addr>` - Sets the address type of the unicast server as Internet Protocol Version 6.
- `domain-name <string(64)>` - Sets the domain name for the unicast server. This value is a string with the maximum size as 64.
- `primary` - Sets the unicast server type as primary server.
- `secondary` - Sets the unicast server type as secondary server.
- `version 3` - Sets the SNTP version as 3.
- `version 4` - Sets the SNTP version as 4.
- `port <integer(1025-36564)`> - Selects the port identifier numbers in the selected server. This value ranges between 1025 and 36564.

Mode SNTP Configuration Mode

Default version 4

Example

```
Your Product (config-sntp)# set sntp unicast-server ipv4 12.0.0.100 Primary
version 3 port 1234
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode
- `show sntp unicast-mode status` - Displays the SNTP Unicast Mode status.
- `show sntp status` – Displays SNTP status.

set sntp broadcast-mode send-request

Command Objective This command either enables or disables the sntp to send status request.

Syntax **set sntp broadcast-mode send-request {enabled | disabled}**

Parameter Description

- `enabled` - Sends the SNTP request packet to broadcast server to calculate the actual delay.

- `disabled` - Does not send any SNTP request packet to broadcast server instead default value for the delay is taken.

Mode SNTP Configuration Mode

Default disabled

Example

```
Your Product (config-sntp)# set sntp broadcast-mode send- request enabled
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode
- `show sntp broadcast-mode status` – Displays the SNTP broadcast mode status.

set sntp broadcast-poll-timeout

Command Objective This command configures SNTP client poll interval in broadcast mode which is the maximum interval to wait for a poll to complete. The value ranges between 1 and 30 seconds.

Syntax **set sntp broadcast-poll-timeout [<value (1-30) seconds>]**

Mode **SNTP Configuration Mode**

Default 5

Example

```
Your Product (config-sntp)# set sntp broadcast-poll-timeout 30
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode
- `show sntp broadcast-mode status` – Displays the SNTP broadcast mode status

set sntp broadcast-delay-time

Command Objective This command configures SNTP delay time in broadcast mode which is the time interval the SNTP client needs to wait for a response from the server. The value ranges between 1000 and 15000 in microseconds.

Syntax **set sntp broadcast-delay-time [<value (1000-15000) microseconds>]**

Mode SNTP Configuration Mode

Default 8000

Example

```
Your Product (config-sntp)# set sntp broadcast-delay-time 2000
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode

- `show sntp broadcast-mode status` – Displays the SNTP broadcast mode status

set sntp multicast-mode send-request

Command Objective This command sets the status of sending the request to the multicast server to calculate the delay time.

Syntax **set sntp multicast-mode send-request {enabled | disabled}**

Parameter Description

- `enabled` - Sends the SNTP request to the multicast server to calculate the actual delay time.
- `disabled` - Does not send any SNTP request to the multicast server.

Mode SNTP Configuration Mode

Default Disabled

Example

```
Your Product (config-sntp)# set sntp multicast-mode send- request enabled
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode
- `show sntp multicast-mode status` – Displays the SNTP multicast mode status

set sntp multicast-poll-timeout

Command Objective This command configures SNTP client poll interval in multicast mode which is the maximum interval to wait for the poll to complete. The value ranges between 1 and 30 seconds.

Syntax **set sntp multicast-poll-timeout [<value (1-30) seconds>]**

Mode SNTP Configuration Mode

Default 5

Example

```
Your Product (config-sntp)# set sntp multicast-poll- timeout 10
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode.
- `show sntp multicast-mode status` – Displays the SNTP multicast mode status.

set sntp multicast-delay-time

Command Objective This command configures SNTP delay time in which there is no response from the multicast server. The value ranges between 1000 and 15000 in microseconds.

Syntax **set sntp multicast-delay-time [<value (1000-15000) microseconds>]**

Mode SNTP Configuration Mode

Default 8000

Example

```
Your Product (config-sntp)# set sntp multicast-delay-time 2000
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode
- `show sntp multicast-mode status` – Displays the SNTP multicast mode status

set sntp multicast-group-address

Command Objective This command configures a group address for the SNTP so that all the SNTP client servers can be connected to this address.

Syntax **set sntp multicast-group-address {ipv4 {<mcast_addr> | default} | ipv6 {<ipv6_addr> | default}}**

Parameter Description

- `ipv4` - Sets the Internet Protocol Version as version 4
  - `<mcast_addr>` - Sets the multicast group address
  - `default`– Sets the multicast default address as a default value
- `ipv6` - Sets the Internet Protocol Version as version 6
  - `< ipv6_addr >` - Sets the ipv6 address
  - `default`– Sets the multicast default address as a default value

Mode SNTP Configuration Mode

Example

```
Your Product (config-sntp)# set sntp multicast-group- address ipv4
224.1.1.10
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode.
- `show sntp multicast-mode status` – Displays the SNTP multicast mode status.

set sntp manycast-poll-interval

Command Objective This command configures SNTP client poll interval which is the maximum interval between successive messages. The poll interval value ranges between 60 and 16284 in seconds.

Syntax **set sntp manycast-poll-interval [<value (60-16284) seconds>]**

Mode SNTP Configuration Mode

Default 64

Example

```
Your Product (config-sntp)# set sntp manycast-poll- interval 60
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode.
- `set sntp client addressing-mode` – Sets the addressing mode of SNTP.
- `show sntp manycast-mode status` – Displays the SNTP manycast mode status.

set sntp manycast-poll-timeout

Command Objective This command configures SNTP client poll timeout which is the maximum interval to wait for a poll to complete. The value ranges between 1 and 30 in seconds.

Syntax **set sntp manycast-poll-timeout [<value (1-30) seconds>]**

Mode SNTP Configuration Mode

Default 5

Example

```
Your Product (config-sntp)# set sntp manycast-poll-timeout 10
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode.
- `set sntp client addressing-mode` – Sets the addressing mode of SNTP
- `show sntp manycast-mode status` – Displays the SNTP manycast mode status.

set sntp manycast-poll-retry-count

Command Objective This command configures SNTP poll retries count which is the maximum number of unanswered polls that cause a slave to identify the server as dead. The value ranges between 1 and 10 in seconds.

Syntax **set sntp manycast-poll-retry-count [<value (1-10)>]**

Mode SNTP Configuration Mode

Default 3

Example

```
Your Product (config-sntp)# set sntp manycast-poll-retry- count 5
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode.
- `set sntp client addressing-mode` – Sets the addressing mode of SNTP

- `show sntp manycast-mode status` – Displays the SNTP manycast mode status

set sntp manycast-server

Command Objective This command configures SNTP multicast or broadcast server address in manycast mode.

Syntax **set sntp manycast-server { broadcast | multicast {ipv4 [<mcast_addr>] |ipv6 [<ip6_addr>]} }**

Parameter Description

- `broadcast` - Configures SNTP broadcast server address in manycast mode
- `multicast` - Configures SNTP multicast server address in manycast mode.
- `ipv4 < mcast_addr>` - Sets the multicast server address in internet protocol v4.
- `ipv6 <ipv6_addr>` - Sets the multicast server address in internet protocol v6.

Mode SNTP Configuration Mode

Example

```
Your Product (config-sntp)# set sntp manycast-server multicast ipv4
224.0.0.1
```

Related Command(s)

- `sntp` - Enters to SNTP configuration mode
- `show sntp manycast-mode status` – Displays the SNTP manycast mode status

show sntp clock

Command Objective This command displays the current time.

Syntax **show sntp clock**

Mode User / Privileged EXEC Mode

Example

```
Your Product# show sntp clock
current time : Sat Jan 01 2000 00:07:04 (UTC + 0: 0 )
```

Related Command(s) `set sntp client clock-format` - Sets the system clock as either AM PM format or HOURS format.

show sntp status

Command Objective This command displays SNTP status.

Syntax **show sntp status**

Mode User / Privileged EXEC Mode

Example

```
Your Product# show sntp status
sntp client is enabled
current sntp client version is v4
current sntp client addressing mode is unicast sntp client port is 123
sntp client clock format is 24 hours sntp client authenticatin key id is 5
sntp client authentication algorithm is md5
sntp client auth Key is Aricent sntp client time zone is + 05:30
sntp client dst start time is not set
sntp client dst end time is not set
```

Related Command(s)

- `set sntp client` – Sends the request to the host for time synchronization.
- `set sntp client version` - Sets the operating version of the client SNTP.
- `set sntp client addressing mode` - Sets the addressing mode of SNTP client.
- `set sntp client port` - Sets the listening port for SNTP client which refers to a port on a server that is waiting for a client connection.
- `set sntp client clock-format` - Sets the system clock as either AM PM / HOURS format.
- `set sntp client authentication-key` - Sets the authentication key for the SNTO clients.
- `set sntp client time-zone` - Sets the system time zone with respect to UTC.
- `sntp client clock-summer-time` - Enables the Daylight Saving Time.
- `show sntp unicast-mode status` – Displays the SNTP Unicast Mode status.
- `show sntp broadcast-mode status` – Displays the SNTP broadcast mode status
- `show sntp multicast-mode status` - Displays the SNTP multicast mode status
- `show sntp manycast-mode status` - Displays the SNTP manycast mode status

show sntp unicast–mode status

Command Objective This command displays the status of SNTP in unicast mode.

Syntax **show sntp unicast-mode status**

Mode User / Privileged EXEC Mode

Note: This command is executed only if the addressing mode is set as unicast.

Example

```
Your Product# show sntp unicast-mode status
auto discovery of sntp/ntp servers is disabled unicast poll interval value is 64
unicast max poll time out value is 5 unicast max retry time value is 3
Unicast current mode value is NOT SYNCHRONIZED
Sntp client is up for 00:03:22
unicast primary server address is 12.0.0.1 unicast primary server version is 4
unicast primary server port is 1056
```

Related Command(s)

- `set sntp client addressing mode` - Sets the addressing mode of SNTP client.
- `set sntp unicast-server auto-discovery` - Configures SNTP client status of auto-discovery of server.
- `set sntp unicast-poll-interval` - Configures SNTP client poll interval.
- `Set sntp unicast-max-poll-timeout` - Configures SNTP client maximum poll interval timeout.
- `set sntp unicast-max-poll-retry` - Configures SNTP client maximum retry poll count.
- `set sntp unicast-server` - Configures SNTP unicast server.
- `show sntp status` - Displays the status of SNTP client.

show sntp broadcast–mode status

Command Objective This command displays the status of SNTP in broadcast mode.

Syntax **show sntp broadcast-mode status**

Mode User / Privileged EXEC Mode

Note: This command is executed only if the addressing mode is set as broadcast.

Example

```
Your Product# show sntp broadcast-mode status
send sntp request to server in broadcast mode is disabled
broadcast poll time out value is 5
broadcast delay time value is 8000
broadcast sntp server is 12.0.0.100
```

Related Command(s)

- `set sntp client addressing mode` - Sets the addressing mode of SNTP client.
- `set sntp broadcast-mode send-request` - Sets the status of sending the request for knowing the delay.
- `set sntp broadcast-poll-timeout` - Configures SNTP client poll interval in broadcast mode.
- `set sntp broadcast-delay-time` - Configures SNTP delay time in broadcast mode.
- `Show sntp status`- Displays the status of SNTP client.

show sntp multicast–mode status

Command Objective This command displays the status of SNTP in multicast mode.

Syntax **show sntp multicast-mode status**

Mode User / Privileged EXEC Mode

Note: If command is executed only if the SNTP client addressing mode is set as multicast.

Example

```
Your Product# show sntp multicast-mode status
send sntp request to server in multicast mode is disabled
multicast poll time out value is 5
multicast delay time value is 8000
multicast group address is 12.0.0.100
```

Related Command(s)

- set sntp client addressing mode - Sets the addressing mode of SNTP client.
- set sntp multicast-mode send-request - Sets the status of sending the request for knowing the delay.
- set sntp multicast-poll-timeout - Configures SNTP client poll interval in multicast mode.
- set sntp multicast-delay-time - Configures SNTP delay time in multicast mode.
- set snto multicast-group-address - Configures SNTP multicast server address.
- show sntp status- Displays the status of SNTP client.

show sntp manycast–mode status

Command Objective This command displays the SNTP manycast mode status.

Syntax **show sntp manycast-mode status**

Mode User / Privileged EXEC Mode

Note: This command executes only if the SNTP client addressing mode is set as manycast.

Example

```
Your Product# show sntp manycast-mode status
manycast poll interval value is 64
manycast max poll time out value is 5
manycast max retry time value is 3
manycast server type is broadcast
primary server address is 12.0.0.100
```

Related Command(s)

- `set sntp client addressing mode` - Sets the addressing mode of SNTP client.
- `set sntp manycast-poll-interval` - Configures SNTP client poll interval in manycast mode.
- `set sntp manycast-poll-timeout` - Configures SNTP client poll timeout in manycast mode.
- `set sntp manycast-poll-retry-count` - Configures SNTP poll retries in manycast mode.
- `set sntp manycast-server`- Configures SNTP multicast or broadcast server address in manycast mode.
- `show sntp status`- Displays the status of SNTP client.

debug sntp

Command Objective This command enables SNTP trace. The no form of the command disables the SNTP trace.

Syntax **debug sntp {all | [init-shut] [mgmt] [data-path] [control] [pkt-dump] [resource] [all-fail] [buff]}**

no debug sntp {all | [init-shut] [mgmt] [data-path] [control] [pkt-dump] [resource] [all-fail] [buff]}

Parameter Description

- `all` - Generates debug statements for all kinds of traces
- `init-shut` - Generates debug statements for init and shutdown traces. This trace is generated on failed initialization and shutting down of SNTP related entries
- `mgmt` - Generates debug statements for management traces. This trace is generated during failure in configuration of any of the SNTP features.
- `data-path` - Generates debug statements for data path traces. This trace is generated during failure in packet processing.
- `control` - Generates debug statements for control path traces. This trace is generated during failure in modification or retrieving of SNTP entries.
- `pkt-dump` - Generates debug statements for packet dump traces. This trace is currently not used in SNTP module.
- `resource` - Generates debug statements for OS resource related traces. This trace is generated during failure in message queues.
- `all-fail` - Generates debug statements for all failure traces of the above mentioned traces.
- `buff` - Generates debug statements for SNTP buffer related traces. This trace is currently not used in SNTP module.

Mode User / Privileged EXEC Mode

Default Debugging is Disabled

Example

```
debug sntp all
```

show sntp statistics

Command Objective This command displays the sntp packet statistics.

Syntax **show sntp statistics**

Mode User / Privilege EXEC Mode

Example

```
Your Product# show sntp statistics
Number of SNTP server-reply Received      : 0
Number of SNTP client-request Transmitted : 0
Number of SNTP Pkt InDiscards             : 0
```

10 SNMPv3

SNMP (Simple Network Management Protocol) is the most widely-used network management protocol on TCP/IP-based networks. SNMPv3 is designed mainly to overcome the security shortcomings of SNMPv1/v2. USM (User based Security Model) and VACM (View based Access Control Model) are the main features added as part of the SNMPv3 specification. USM provides both encryption and authentication of the SNMP PDUs, while VACM specifies a mechanism for defining access policies for different users with different MIB trees. Also, SNMPv3 specifies a generic management framework, which is expandable for adding new

Management Engines, Security Models, Access Control Models and so on. With SNMPv3, the SNMP communication is completely safe and secure.

The list of CLI commands for the configuration of SNMPv3 is as follows:

- enable snmpsubagent
- disable snmpsubagent
- enable snmpagent
- disable snmpagent
- snmp community index
- snmp group
- snmp access
- snmp engineid
- snmp proxy name
- snmp mibproxy name
- snmp view
- snmp targetaddr
- snmp targetparams
- snmp user
- snmp notify
- snmp filterprofile
- snmp-server enable traps snmp authentication
- snmp-server trap udp-port
- snmp-server trap proxy-udp-port
- snmp agent port
- snmp tcp enable
- snmp trap tcp enable

- snmp-server tcp-port
- snmp-server trap tcp-port
- snmp-server enable traps
- show snmp agentx information
- show snmp agentx statistics
- show snmp
- show snmp community
- show snmp group
- show snmp group access
- show snmp engineID
- show snmp proxy
- show snmp mibproxy
- show snmp viewtree
- show snmp targetaddr
- show snmp targetparam
- show snmp user
- show snmp notif
- show snmp inform statistics
- show snmp-server traps
- show snmp-server proxy-udp-port
- show snmp tcp
- show snmp filter
- snmpset mib
- snmpget mib
- snmpgetnext mib
- snmpwalk mib
- snmp filter trap
- show mib oid
- show mib name

enable snmpsubagent

Command Objective This command configures the SNMP to act as a snmp agentx-subagent and also configures the master agent parameters

Syntax **enable snmpsubagent { master { ip4 <ipv4_address> | ip6 <ipv6_address> } [port <number>] }**

Parameter Description

- `master` - Registers all the master agent information and agent capabilities after successful index allocation.
- `ip4<ipv4_address>`- Configures the ip address of the master agent with the given v4 IP address.
- `ip6<ipv6_address>`- Configures the ip address of the master agent with the given v6 IP address.

- `port<number>` - Sets the master port number through which the Agentx PDUs are transmitted to the master agent.

Mode Global Configuration Mode

Default port - 705

Note: This Example is executable only if snmp agent is disabled.

Example

```
Your Product (config)# enable snmpsubagent master ip4 10.0.0.5 port 897
```

Related Command(s)

- `disable snmpsubagent` - Disables agentx-subagent
- `disable snmpagent` - Disables SNMP agent.
- `enable snmpagent` - Enables SNMP agent.
- `show snmp agentx information` - Displays global information of SNMP Agentx communications.
- `show snmp agentx statistics` - Displays all the information regarding SNMP Agentx statistics.

disable snmpsubagent

Command Objective This command disables agentx-subagent.

Syntax **disable snmpsubagent**

Mode Global Configuration Mode

Example

```
Your Product (config)# disable snmpsubagent
```

Related Command(s)

- `enable snmpsubagent` - Enables agentx-subagent capabilities.
- `show snmp agentx information` - Displays global information of SNMP Agentx communications.
- `show snmp agentx statistics`- Displays all the information regarding SNMP Agentx statistics.

enable snmpagent

Command Objective This command enables SNMP agent, which provides an interface between a SNMP manager and a switch. The agent processes SNMP packets received from the manager, frames the appropriate response packets and sends them to the manager.

Syntax **enable snmpagent**

Mode Global Configuration Mode

Default SNMP agent is enabled.

Example

```
Your Product (config)# enable snmpagent
```

Related Command(s)

- `enable snmpsubagent` - Enables agentx-subagent capabilities.
- `disable snmpagent` - Disables SNMP agent.

disable snmpagent

Command Objective This command disables SNMP agent.

Syntax **disable snmpagent**

Mode Global Configuration Mode

Example `Your Product (config)# disable snmpagent`

Related Command(s)

- `enable snmosubagent` - Enables either snmp agent or agentx-subagent capabilities.
- `enable snmpagent` - Enables SNMP agent.
- `show snmp agentx statistics` - Displays all the information regarding SNMP Agentx statistics.

snmp community index

Command Objective This command configures the SNMP community details. The no form of this command removes the SNMP community details.

Syntax **snmp community index <CommunityIndex> name <CommunityName> security <SecurityName> [context <Name >][{volatile | nonvolatile}] [transporttag <TransportTagIdentifier | none>] [contextengineid <ContextEngineID>]**

no snmp community index <CommunityIndex>

Parameter Description

- `<CommunityIndex>` - Creates a community index identifier which stores the index value of the row. This ID must be unique for every community name entry.
- `name<CommunityName>` - Creates a community name which stores the community string.
- `security<SecurityName>` - Stores the security model of the corresponding Snmp community name.
- `Context <Name>` - Indicates the name of the context in which the management information is accessed when using the community string specified by the corresponding instance of snmp community name
- `volatile | nonvolatile` - Sets the storage type as either volatile or non volatile.
  - volatile – Sets the storage type as temporary and erases the configuration setting on restarting the system.

  - nonvolatile – Sets the storage type as permanent and saves the configuration to the system. The saved configuration can be viewed on restarting the system.
- `<TransportTagIdentifier>` - Specifies a set of transport endpoints from which a command responder application can accept management request.
- `contextengineid<ContextEngineID>` - Indicates the location of the context through which the management information is accessed when using the community string specified by the corresponding instance of snmp community name

Mode Global Configuration Mode

Default

- Community Index - NETMAN/PUBLIC
- CommunityName - NETMAN/PUBLIC
- Security Name - None
- ContextName - Null
- Context EngineID - 80.00.08.1c.04.46.53
- Transport Tag - Null
- Storage type - Non Volatile
- Row Status - Active

Example

```
Your Product (config)# snmp community index myv3com name myv3com security
xyz context myinst nonvolatile transporttag myv3tag
```

Related Command(s)

- `show snmp` - Displays the status information of SNMP communications
- `show snmp community` - Displays the configured SNMP community details

snmp group

Command Objective This command configures SNMP group details.

The no form of the command removes the SNMP group details.

Syntax **snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3 } [{volatile | nonvolatile}]**

no snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3 }

Parameter Description

- `<GroupName>` - Creates a name for an SNMP group
- `user<UserName>` - Sets an user for the configured group.
- `security-model` - Sets the security model for SNMP
  - `v1` - Sets the SNMP version as Version 1.
  - `v2c` - Sets the SNMP version as Version 2.

    - v3 - Sets the SNMP version as Version 3.
- volatile | nonvolatile - Sets the required storage type for the group entry
    - volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system.
    - nonvolatile – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.

Mode Global Configuration Mode

Default

- Security model - V3
- Security Name - none / initial / templateMD5 / templateSHA
- Group Name - iso/initial
- Storage Type - non volatile
- Row status - Active

Example

```
Your Product (config)# snmp group myv3group user myv3user security-model v1
volatile
```

Related Command(s)

- snmp access - Configures the SNMP group access details
- show snmp group - Displays the configured SNMP groups
- show snmp user - Displays the configured SNMP users
- show snmp group - Displays the configured SNMP groups.

snmp access

Command Objective This command configures the SNMP group access details. To configure an SNMP access along with the group, a group must have already been created using the snmp group command. The no form of the command removes the SNMP group access details.

Syntax **snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}} [read <ReadView | none>] [write <WriteView | none>] [notify <NotifyView | none>] [{volatile | nonvolatile}] [context <string(32)>]**

no snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}

Parameter Description

- <GroupName> - Sets the name of the group for which access is to be provided.
- v1 | v2c | v3- Sets the SNMP verison.
    - v1– Sets the SNMP version as Version 1.
    - v2c– Sets the SNMP version as Version 2.

    - `v3` – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word
- `auth` - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication.
- `noauth` - Sets no-authentication
- `priv` - Sets both authentication and privacy
- `read`- Mentions the MIB view of the SNMP context to which read access is authorized by this entry
- `write` - Mentions the MIB view of the SNMP context to which write access is authorized by this entry
- `notify` - Mentions the MIB view of the SNMP context to which notification access is authorized by this entry
- `volatile | nonvolatile` - Sets the required storage type for the group entry
    - `volatile` – Sets the storage type as temporary. Erases the configuration setting on restarting the system.
    - `nonvolatile` – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.
- `context<string(32)>` - Configures the name of the SNMP context. The maximum length of the string is 32.

Mode Global Configuration Mode

Default

- Group Name - iso
- Read/Write/Notify view - iso
- Storage Type - volatile
- Row status - Active
- Group Name - initial
- Read/Write/Notify View - restricted
- Storage Type - non-volatile
- Group Name - Initial
- Read/Write/Notify View - iso
- Storage Type - non-volatile

Example

```
Your Product (config)# snmp access myv2group v2 read v2readview write
v2writeview notify v2notifyview nonvolatile
```

Related Command(s)

- `snmp group` - Configures SNMP group details
- `snmp view` - Configures the SNMP view
- `show snmp group` - Displays the configured SNMP groups
- `show snmp group access` - Displays the configured SNMP group access details
- `show snmp viewtree` - Displays the configured SNMP Tree views

snmp engineid

Command Objective This command configures the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to coordinate the exchange of messages between the source and the destination.

The no form of the command resets the engine ID to the default value.

Syntax

snmp engineid <EngineIdentifier>

no snmp engineid

Mode Global Configuration Mode

Default 80.00.08.1c.04.46.53

- The Engine ID must be given as octets in hexadecimal separated by dots and the allowed length is 5 to 32 octets.
- SNMP engine ID is an administratively unique identifier.
- Changing the value of the SNMP engine ID has significant effects.
- All the user information will be updated automatically to reflect the change

Example

```
Your Product (config)# snmp engineid 80.0.08.1c.04.5f.a9
```

Related Command(s)

- `show snmp engineID` - Displays the Engine Identifier
- `show snmp user` - Displays the configured SNMP users

snmp proxy name

Command Objective This command configures the proxy.
The no form of the command removes the proxy.

Syntax **snmp proxy name <ProxyName> ProxyType {Read | Write | inform | Trap} ContextEngineID <EngineId> TargetParamsIn <TargetParam> TargetOut <TargetOut> [ContextName <ProxyContextName>] [StorageType {volatile | nonvolatile}]**

no snmp proxy name <ProxyName>

Parameter Description

- <ProxyName> - Identifies an entry in the proxy table.
    - This will be the INDEX used for the Proxy Table.
- ProxyType - Forwards the messages using the translation parameters defined by proxy entry. The

list contains:. Options are:

  - Read – Forwards the read messages to get the request from the manager.
  - Write – Forwards the write messages toset configurations.
  - Inform – Forwards the notification messages to theagent.
  - Trap – Forwards the SNMP trap messages to theagent

- ContextEngineID <EngineId> - Configures an context engine ID of the agent with whom the manager communicates through the proxy.
- TargetParamsIn <TargetParam> - Configures the SNMP version that the manager sends as request to the proxy.
- TargetOut <TargetOut> - Configures the SNMP version that the proxy uses to communicate with multiple agent.
  - This object is only used when selection of a single target is required (that is, when forwarding an incoming read or write request).
- ContextName <ProxyContextName> - Configures an unique context name for an SNMP sub agent. This name is used to identify the corresponding sub agent when more than one sub agent exists.
- Storage Type - Sets the required storage type for the group entry
  - volatile –Sets the storage type as temporary. Erases the configuration setting on restarting the system.
  - nonvolatile – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.

Mode Global Configuration Mode

Default Storage Type - Nonvolatile

Example

```
Your Product (config)# snmp proxy name proxy1 ProxyType write
ContextEngineID 80.00.08.1c.04.46.53 TargetParamsIn param2 TargetOut
target2 ContextName pxyctxtname StorageType nonvolatile
```

Related Command(s)

- `show snmp group` - Displays the configured SNMP groups
- `show snmp proxy` - Displays proxy details.

snmp mibproxy name

Command Objective This command configures the mib proxy. The no form of the command removes the mib proxy.

Syntax **snmp mibproxy name <ProxyName> ProxyType {Read | Write | inform | Trap} mibid <MibId> TargetParamsIn <TargetParam> TargetOut <TargetOut> [StorageType {volatile | nonvolatile}]**

no snmp mibproxy name <ProxyMibName>

Parameter Description

- `<ProxyName>` - Identifies an entry in the proxy table
  - This will be the INDEX used for the Proxy Table.
- `ProxyType` - Forwards the messages using the translation parameters defined by proxy entry. The list contains:. Options are:
  - `Read`– Forwards the read messages to get the request from the manager.
  - `Write`– Forwards the write messages to set configurations.
  - `Inform`– Forwards the notification messages to the agent.
  - `Trap`– Forwards the SNMP trap messages to the agent
- `Mibid <MibId>` - Configures a context MIB ID of the agent with whom the manager communicates through the proxy.
- `TargetParamsIn<TargetParam>` - Configures the SNMP version that the manager sends as request to the proxy.
- `TargetOut<TargetOut>` - Configures the SNMP version that the proxy uses to communicate with multiple agent .This object is only used when selection of a single target is required (that is, when forwarding an incoming read or write request).
- `Storage Type` - Storage type. Options are:
  - `volatile` – Sets the storage type as temporary. Erases the configuration setting on restarting the system.
  - `nonvolatile` – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.

Mode Global Configuration Mode

Example

```
Your Product (config)# snmp mibproxy name mibproxy1 ProxyType read mibid 1
TargetParamsIn param1 TargetOut target1 StorageType nonvolatile
```

Related Command(s)

- `show snmp group` - Displays the configured SNMP groups
- `show snmp mibproxy` - Displays the mib proxy details.

snmp view

Command Objective This command configures the SNMP view. The no form of the command removes the SNMP view.

Syntax **snmp view <ViewName> <OIDTree> [mask <OIDMask>] {included| excluded} [{volatile | nonvolatile}]**

no snmp view <ViewName> <OIDTree>

Parameter Description

- `<ViewName>` - Specifies the view name for which the view details are to be configured. This is a string value with maximum size as 32.
- `<OIDTree>` - Specifies the sub tree value for the particular view.
- `mask <OIDMask>` - Specifies a mask value for the particular view.
- `included` - Allows access to the subtree
- `excluded` - Denies access to the subtree
- `volatile` - Sets the storage type as temporary. Erases the configuration setting on restarting the system.
- `nonvolatile` - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system.

Mode Global Configuration Mode

Default

- View Name - iso/restricted
- OIDTree - 1
- OIDMask - 1
- View type - included
- Storage type - non-volatile
- Row status - Active
    - To configure an SNMP view (read/write/notify), a group must have already been created using the snmp group command and SNMP group access must be configured using the snmp access command.

Example

```
Your Product (config)# snmp view v2readview 1.3.6.1 mask 1.1.1.1 included
nonvolatile
```

Related Command(s)

- `snmp access` - Configures the SNMP group access details
- `show snmp viewtree` - Displays the configured SNMP Tree views
- `show snmp group access` - Displays the configured SNMP group access details

snmp targetaddr

Command Objective This command configures the SNMP target address.
The no form of the command removes the configured SNMP target address.

Syntax **snmp targetaddr <TargetAddressName> param <ParamName> {<IPAddress> | <IP6Address>} [timeout <Seconds(1-1500>] [retries <RetryCount(1-3)] [taglist <TagIdentifier | none>] [{volatile | nonvolatile}] [port <integer (1-65535)>]**

no snmp targetaddr <TargetAddressName>

Parameter Description

- `<TargetAddressName>` - Configures a unique identifier of the Target.
- `param<ParamName>` - Configures the parameters when generating messages to be sent to transport address.
- `IPAddress` - Configures an IP target address to which the generated SNMP notifications are sent.
- `IP6Address` - Configures an IP6 target address to which the generated SNMP notifications are sent.
- `timeout<Seconds(1-1500)>` - Sets the time in which the SNMP agent waits for a response from the SNMP Manager before retransmitting the Inform Request Message. The value ranges between 1 and 1500 seconds.
- `retries<RetryCount(1-3)>` - Sets the maximum number of times the agent can retransmit the Inform Request Message. This value ranges between 1 and 3.
- `taglist<TagIdentifier | none>` - Sets the tag identifier that selects the target address for the SNMP. The taglist can also be set as none using the none option.
- `volatile` - Sets the storage type as temporary. Erases the configuration setting on restarting the system
- `nonvolatile` - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system.
- `port <integer (1-65535)>` - Configures a port number through which the generated SNMP notifications are sent to the target address. The value ranges between 1 and 65535.

Mode Global Configuration Mode

Default

- ParamName - Internet
- IPAddress - 10.0.0.10
- taglist - snmp
- volatile | nonvolatile - volatile
- port - 162
    - Target param must have been configured.

Example

```
Your Product (config)# snmp targetaddr smismgr param smisd 10.0.0.10
taglist mytag nonvolatile
```

Related Command(s)

- `snmp targetparams` - Configures the SNMP target parameters
- `show snmp targetaddr` - Displays the configured SNMP target Addresses
- `show snmp targetparam` - Displays the configured SNMP Target Address Params

snmp targetparams

Command Objective This command configures the SNMP target parameters. The no form of the command removes the SNMP target parameters.

Syntax **snmp targetparams <ParamName> user <UserName> security- model {v1 | v2c | v3 {auth | noauth | priv}} message- processing {v1 | v2c | v3} [{volatile | nonvolatile}] [filterprofile-name <profilename>] [filter-storagetype {volatile | nonvolatile}]**

no snmp targetparams <ParamName>

Parameter Description

- `<ParamName>` - Sets a unique identifier of the parameter.
- `User <UserName>` - Sets a user for which the target parameter is to be done.
- `security-model` - Sets the security model
- `v1` – Sets the SNMP version as Version 1.
- `v2c` – Sets the SNMP version as Version 2.
- `v3` – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word
- `auth` - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication
- `noauth` - Sets no-authentication
- `priv` - Specifies both authentication and privacy
- `message-processing` - Sets the message processing model
  - v1 **–** Sets the SNMP version as Version 1.
  - v2c **–** Sets the SNMP version as Version 2.
  - v3 **–** Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word
- `volatile` - Sets the storage type as temporary. Erases the configuration setting on restarting the system
- `nonvolatile` - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system.
- filterprofile-name <profilename> - Configures the profile name
- filter-storagetype - Sets the required storage type for the filter profile
  - volatile **–** Sets the storage type as temporary. Erases the configuration setting on restarting the system.
  - nonvolatile **–** Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.

Mode Global Configuration Mode

Default

- Target ParamName - internet
- User/Security Name - None
- Security Model - v2c

- Security Level - NoauthNoPriv
- Message Processing Model - v2c
- Storage Type - Non-volatile
- Row status - Active
- Filter profile name - None
- ParamName - test1
- User/Security Name - None
- Security Model - v1
- Security Level - NoauthNoPriv
- Message Processing Model - v1
- Storage Type - Non-volatile
- Row status - Active
- Filter profile name - None

Note: User information must have been configured prior to the configuration of SNMP target **parameters**

Example

```
Your Product (config)# snmp targetparams param1 user user1 security-model
v3 noauth message-processing v3
```

Related Command(s)

- `snmp user` - Configures the SNMP user details
- `snmp targetaddr` - Configures the SNMP target address
- `show snmp targetparam` - Displays the configured SNMP Target Address Params
- `show snmp user` - Displays the configured SNMP users.
- `show snmp notif` - Displays the configured SNMP Notifications

snmp user

Command Objective This command configures the SNMP user details.

The no form of the command removes the SNMP user details.

Syntax **snmp user <UserName> [auth {md5 | sha} <passwd> [priv {{{DES | AES_CFB128} <passwd> } | None}]] [{volatile | nonvolatile}] [EngineId <EngineID>]**

no snmp user <UserName> [EngineId <EngineID>]

Parameter Description

- `<UserName>` - Configures an user name which is the User-based Security Model dependent security ID.
- `auth` - Sets an authentication Algorithm . Options are:
  - `md5` - Sets the Message Digest 5 based authentication.
  - `sha` - Sets the Security Hash Algorithm based authentication.

- `<Passwd>` - Sets the authentication password that will be used for the configured authentication algorithm.
- `priv` - Sets the DES encryption and also the password to be used for the encryption key. Options are:
    - `DES` – Configures the data encryption standard algorithm related configuration.
    - `AES_CFB128` – Configures Advanced Encryption Standard (AES) algorithm for encryption.
    - `<Passwd>` - Sets the authentication password that will be used for the configured authentication algorithm.
    - `None` - Sets encryption configuration as none.
- `volatile` - Sets the storage type as temporary. Erases the configuration setting on restarting the system
- `nonvolatile` - Sets the storage type as permanent. Saves the configuration to the system. You can view the saved configuration on restarting the system
- `EngineId <EngineID>` - Sets the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to coordinate the exchange of messages between the source and the destination.

Mode Global Configuration Mode

Default

- UserName - Initial
- Authentication Protocol - None
- Privacy Protocol - None
- Storage type - Non-volatile

Note: SNMP passwords are localized using the local SNMP engine ID

Example

```
Your Product (config)# snmp user user1
```

Related Command(s)

- `show snmp engineID` - Displays the Engine Identifier
- `show snmp user` - Displays the configured SNMP users
- `snmp targetparams` - Configures the SNMP target parameters
- `show snmp group` - Displays the configured SNMP groups

snmp notify

Command Objective This command configures the SNMP notification details.

The no form of this command removes the SNMP notification details.

Syntax **snmp notify <NotifyName> tag <TagName> type {Trap | Inform} [{volatile | nonvolatile}]**

no snmp notify <NotifyName>

Parameter Description

- `<NotifyName>` - Configures an unique identifier associated with the entry.
- `tag<TagName>` - Sets a notification tag, which selects the entries in the Target Address Table.
- `type` - Sets the notification type. The list contains:
  - `Trap` – Allows routers to send traps to SNMP managers. Trap is a one-way message from a network element such as a router, switch or server; to the network management system.
  - `Inform`– Allows routers / switches to send inform requests to SNMP managers
- `volatile` - Sets the storage type as temporary. Erases the configuration setting on restarting the system.
- `nonvolatile` - Sets the storage type as permanent. Saves the configuration to the system. You can view the Saved configuration on restarting the system

Mode Global Configuration Mode

Default

- Notify Name - smis1
- Notify Tag - smis1
- Storage type - volatile

Example

```
Your Product (config)# snmp notify note1 tag tag1 type Inform
```

Related Command(s)

- `show snmp notif` - Displays the configured SNMP Notifications
- `show snmp targetaddr` - Displays the configured SNMP target Addresses

snmp filterprofile

Command Objective This command creates Notify filter Profile entry.

The no form of the command removes the filter entry from the table.

Syntax **snmp filterprofile <profile-name> <OIDTree> [mask <OIDMask>] {included | excluded} [{volatile | nonvolatile}]**

no snmp filterprofile <profilename> <OIDTree>

Parameter Description

- `profile-name` - Configures the name of the filter profile. This is a string value with a maximum size as 32.
- `OIDTree` - Configures the object Identifier

- `mask <OIDMask>` - Defines a family of subtrees, in combination with the object identifier.
- `included | excluded` - Configures the type of filter. This indicates whether the family of subtrees defined by the OID and mask should be included in or excluded from the filter profile.
- `volatile | nonvolatile` - Specifies the storage type. The list contains;
    - `volatile` - Temporary storage. Details are lost once restarted.
    - `nonvolatile` - Permanent storage. Details are present even after restart.

Mode Global Configuration Mode

Example

```
Your Product (config)# snmp filterprofile filter1 1.5 mask1.1 included
nonvolatile
```

Related Command(s)

- `show snmp filter` - Displays the configured SNMP filters
- `snmp targetparams` - Configures the SNMP target parameters

snmp-server enable traps snmp authentication

Command Objective This command enables generation of authentication traps from the snmp agent (for all snmpv1, snmpv2 and snmpv3).

The no form of the command disables generation of authentication traps.

Syntax **snmp-server enable traps snmp authentication**

no snmp-server enable traps snmp authentication

Mode Global Configuration Mode

Default Disabled

Example

```
Your Product (config)# snmp-server enable traps snmp authentication
```

snmp-server trap udp-port

Command Objective This command configures the udp port over which agent sends the trap.

The no form of the command configures the snmp agent to send trap on default udp port.

Syntax **nmp-server trap udp-port <port>**

no snmp-server trap udp-port

Mode Global Configuration Mode

Example Your Product (config)# snmp-server trap udp-port 1234

Related Command(s) `show snmp notif` - Displays the configured SNMP Notification types.

snmp-server trap proxy-udp-port

`Command Objective` This command configures the udp port over which agent sends the trap to the proxy entity.

The no form of the command configures the snmp agent to send trap on default udp port.

Syntax **snmp-server trap proxy-udp-port <port>**

no snmp-server trap proxy-udp-port

Mode Global Configuration Mode

Default 162

Example

```
Your Product (config)# snmp-server trap proxy-udp-port 162
```

Related Command(s) `show snmp-server proxy-udp-port` - Displays the proxy udp port.

snmp agent port

Command Objective This command configures the agent port on which agent listens.

The port number value ranges between 1 and 65535.

Syntax **snmp agent port <port>**

Mode Global Configuration Mode

Default 161

Example

```
Your Product (config)# snmp agent port 100
```

Related Command(s) `show snmp` - Displays the status information of SNMP communications

snmp tcp enable

Command Objective This command enables sending snmp messages over tcp.

The no form of the command disables sending snmp messages over tcp.

Syntax **snmp tcp enable**

no snmp tcp enable

Mode Global Configuration Mode

Default Disabled

Example `Your Product (config)# snmp tcp enable`

Related Command(s) `show snmp tcp` - Displays the configuration for snmp over tcp.

snmp trap tcp enable

Command Objective This command enables sending snmp trap messages over tcp.

The no form of the command disables sending snmp trap messages over tcp.

Syntax **snmp trap tcp enable**

no snmp trap tcp enable

Mode Global Configuration Mode

Default Disabled

Example `Your Product (config)# snmp trap tcp enable`

Related Command(s) `show snmp tcp` - Displays the configuration for snmp over tcp.

snmp-server tcp-port

Command Objective This command configures the tcp port over which agent sends the snmp message. This value ranges between 1 and 65535.

The no form of the command configures the snmp agent to send snmp message on default tcp port.

Syntax **snmp-server tcp-port <port>**

no snmp-server tcp-port

Mode Global Configuration Mode

Default 161

Example `Your Product (config)# snmp-server tcp-port 161`

Related Command(s) `show snmp tcp` - Displays the configuration for snmp over tcp.

snmp-server trap tcp-port

Command Objective This command configures the tcp port over which agent sends the trap. Thisvalue ranges between 1 and 65535.

The no form of the command configures the snmp agent to send trap on default tcp port.

Syntax **snmp-server trap tcp-port <port>**

no snmp-server trap tcp-port

Mode Global Configuration Mode

Default 162

Example

```
Your Product (config)# snmp-server trap tcp-port 162
```

Related Command(s) `show snmp tcp` - Displays the configuration for snmp over tcp.

snmp-server enable traps

Command Objective This command enables generation of a particular trap.

The no form of the command disables generation of a particular trap.

Syntax **snmp-server enable traps {[firewall-limit] [linkup] [linkdown] [sip-states] [sip-cfg-change] [coldstart] [poe- power] [dhcp-pool-limit] [dsx1-line]}**

no snmp-server enable traps {[firewall-limit] [linkup] [linkdown] [sip-states] [sip-cfg-change] [coldstart] [poe- power] [dhcp-pool-limit] [dsx1-line]}

Parameter Description

- `firewall-limit` - Generates a trap for all the firewall attack summary
- `linkup` - Generates a trap whenever there is a linkup
- `linkdown` - Generates a trap whenever there is a linkdown
- `sip-states` - Generates a trap for all the SIP states .
- `sip-cfg-change` - Generates a trap for all the SIP configuration
- `coldstart` - Generates a trap for all the Coldstart
- `poe-power` - Generates a trap whenever there is Power on Ethernet
- `dhcp-pool-limit` - Generates a trap for all the DHCP server pool limit trap
- `dsx1-line` - Generates a trap for all the DSX1 line trap

Mode Global Configuration Mode

Example

```
Your Product (config)# snmp-server enable traps firewall- limit
```

Related Command(s) `show snmp-server traps` - Displays the set of traps that are currently enabled.

show snmp agentx information

Command Objective This command displays global information of SNMP Agentx communications.

Syntax **show snmp agentx information**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp agentx information
Agentx Subagent is enabled TransportDomain  :TCP
Master IP Address :10.0.0.2
Master PortNo     705
```

Related Command(s)

- `enable snmpsubagent` - Enables agentx-subagent capabilities.
- `disable snmpsubagent` - Disables agentx-subagent.
- `disable snmpagent` - Disables SNMP agent.

show snmp agentx statistics

Command Objective This command displays all the information regarding SNMP Agentx statistics.

Syntax **show snmp agentx statistics**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp agentx statistics
Tx Statistics
    Transmitted Packets                  860
    Open PDU                             1
    Index Allocate PDU                   0
    Index DeAllocate PDU                 0
    Register PDU                         2
    Add Agent Capabilities PDU           0
    Notify PDU                           0
    Ping PDU                             20
    Remove Agent Capabilities PDU        0
    UnRegister PDU                       0
    Close PDU                            0
    Response PDU                         837
Rx Statistics
    Rx Packets                          :859
    Get PDU                             :1
    GetNext PDU                         :836
    GetBulk PDU                         :0
    TestSet PDU                         :0
    Commit PDU                          :0
    Cleanup PDU                         :0
    Undo PDU                            :0
    Dropped Packets                     :0
    Parse Drop Errors                   :1
    Open Fail Errors                    :0
    Close PDU                           :0
    Response PDU                        :21
```

Related Command(s)

- `enable snmpsubagent` - Enables agentx-subagent capabilities.
- `disable snmpsubagent` - Disables agentx-subagent.
- `disable snmpagent` - Disables snmp agent

show snmp

Command Objective This command displays the status information of SNMP communications.

Syntax **show snmp**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp
  0 SNMP Packets Input
    0 Bad SNMP Version errors
    0 Unknown community name
    0 Get request PDUs
    0 Get Next PDUs
    0 Set request PDUs
  0 SNMP Packets Output
    0 Too big errors
    0 No such name errors
    0 Bad value errors
    0 General errors
    0 Trap PDUs
  0 SNMP Rollback failures
SNMP Manager-role output packets
    0 Drops
SNMP Informs:
    0 Inform Requests generated
    0 Inform Responses received
    0 Inform messages Dropped
    0 Inform Requests awaiting Acknowledgement
SNMP Trap Listen Port is 162
snmp agent port : 170
```

Related Command(s) `snmp community index` - Configures the SNMP community details

show snmp community

Command Objective This command displays the configured SNMP community details.

Syntax **show snmp community**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp community
Community Index: NETMAN Community Name: NETMAN Security Name: none Context
Name:
Transport Tag:
Storage Type: volatile
Row Status: active
------------------------------------------------
Community Index: PUBLIC
Community Name: PUBLIC
Security Name: none
Context Name: Transport Tag:
Storage Type: volatile
Row Status: active
```

Related Command(s) `snmp community index` - Configures the SNMP community details

show snmp group

Command Objective This command displays the configured SNMP groups.

Syntax **show snmp group**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp group
Security Model: v1
Security Name: none
Group Name: iso
Storage Type: volatile
Row Status: active
------------------------------------------------
Security Model: v2c
Security Name: none
Group Name: iso

Storage Type: volatile
Row Status: active
------------------------------------------------
Security Model: v3
Security Name: initial
Group Name: initial
Storage Type: nonvolatile
Row Status: active
------------------------------------------------
Security Model: v3
Security Name: templateMD5
Group Name: initial
Storage Type: nonvolatile
Row Status: active
------------------------------------------------
```

```
Security Model: v3
Security Name: templateSHA
Group Name: initial
Storage Type: nonVolatile
Row Status: active
```

Related Command(s)

- `snmp group` - Configures the SNMP group details
- `snmp access` - Configures the SNMP group access details
- `snmp user` - Configures the SNMP user details
- `snmp proxy name` - Configures the proxy.
- `snmp mibproxy name` - Configures the mibproxy.

show snmp group access

Command Objective This command displays the configured SNMP group access details.

Syntax **show snmp group access**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp group access
Group Name: iso Read View: iso Write View: iso Notify View: iso
Storage Type: volatile
Row Status: active
------------------------------------------------
Group Name: iso
Read View: iso Write View: iso Notify View: iso
Storage Type: volatile
Row Status: active
------------------------------------------------
Group Name: initial
Read View: restricted
Write View: restricted
Notify View: restricted
Storage Type: nonVolatile
Row Status: active
------------------------------------------------
Group Name: initial
Read View: iso Write View: iso Notify View: iso
Storage Type: nonVolatile
Row Status: active
```

Related Command(s)

- `snmp access` - Configures the SNMP group access details
- `snmp view` - Configures the SNMP view

show snmp engineID

Command Objective This command displays the Engine Identifier.

Syntax **show snmp engineID**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp engineID
EngineId: 80.00.08.1c.04.46.53
```

Related Command(s)

- `snmp engineid` - Configures the engine identifier
- `snmp user` - Configures the SNMP user details

show snmp proxy

Command Objective This command displays proxy details.

Syntax **show snmp proxy**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp proxy
Proxy Name                : PROXY1
Proxy ContextEngineID     : 80.00.08.1c.04.46.54
Proxy ContextName         :
Proxy TargetParamIn       : param1
Proxy SingleTargetOut     : Tgt1
Proxy MultipleTargetOut   :
Proxy Type                : Read
Storage Type              : Non-volatile
Row Status                : Active
----------------------------------------------------------------------------
Proxy Name                : PROXY2
Proxy ContextEngineID     : 80.00.08.1c.04.46.54
Proxy ContextName         :
Proxy TargetParamIn       : param1
Proxy SingleTargetOut     : Tgt1
Proxy MultipleTargetOut   :
Proxy Type                : Write
Storage Type              : Non-volatile
Row Status                : Active
```

Related Command(s) `snmp proxy name` - Configures the proxy.

show snmp mibproxy

Command Objective This command displays proxy details.

Syntax **show snmp mibproxy**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp mibproxy
Prop Proxy Name                 : proxy1
Prop MibID                      : 2
Prop Proxy TargetParamIn        : param1
Prop Proxy SingleTargetOut      : target1
Prop Proxy MultipleTargetOut    :
Prop Proxy Type                 : Read
Prop Storage Type               : Non-volatile
Prop Row Status                 : Active
-------------------------------------------------------------------------------
```

Related Command(s) `snmp mibproxy name` - Configures the proxy.

show snmp viewtree

Command Objective This command displays the configured SNMP Tree views.

Syntax **show snmp viewtree**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp viewtree
View Name: iso
Subtree OID: 1
Subtree Mask:
View Type: included Storage Type: nonVolatile Row Status: active
---------------------------------------------- View Name: restricted
Subtree OID: 1
Subtree Mask:
View Type: included Storage Type: nonVolatile Row Status: active
----------------------------------------------
```

Related Command(s)

- `snmp access` - Configures the SNMP group access details
- `snmp view` - Configures the SNMP view

show snmp targetaddr

Command Objective This command displays the configured SNMP target Addresses.

Syntax **show snmp targetaddr**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp targetaddr
Target Address Name : ht231
IP Address          : 12.0.0.100
Port                : 150
Tag List            : tg231
Parameters          : pa231
Storage Type        : Non-volatile
Row Status          : Active
------------------------------------------------
```

Related Command(s)

- `snmp targetaddr` - Configures the SNMP target address
- `snmp targetparams` - Configures the SNMP target parameters
- `snmp notify` - Configures the SNMP notification details

show snmp targetparam

Command Objective This command displays the configured SNMP Target Address Params.

Syntax **show snmp targetparam**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp targetparam
Target Parameter Name    : internet
Message Processing Model : v2c
Security Model           : v2c
Security Name            : none
Security Level           : No Authentication, No Privacy
Storage Type             : Non-volatile
Row Status               : Active
Filter Profile Name      : None
Row Status               : Active
------------------------------------------------
Target Parameter Name    : pa231
Message Processing Model : v3
Security Model           : v3
Security Name            : u231
Security Level           : No Authentication, No Privacy
Storage Type             : Volatile
Row Status               : Active
```

```
Filter Profile Name     : filter1
Row Status              : Active
-----------------------------------------------
Target Parameter Name   : test1
Message Processing Model : v2c
Security Model          : v1
Security Name           : none
Security Level          : No Authentication, No Privacy
Storage Type            : Non-volatile
Row Status              : Active
Filter Profile Name     : None
Row Status              : Active
-------------------
```

Related Command(s)

- `snmp targetaddr` - Configures the SNMP target address
- `snmp targetparams` - Configures the SNMP target parameters
- `snmp user` - Configures the SNMP user details

show snmp user

Command Objective This command displays the configured SNMP users.

Syntax **show snmp user**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp user
Engine ID: 80.00.08.1c.04.46.53
User: initial
Authentication Protocol: non
Privacy Protocol: none
Storage Type: nonVolatile
Row Status: active
-----------------------------------------------
Engine ID: 80.00.08.1c.04.46.53
User: templateMD5
Authentication Protocol: MD5
Privacy Protocol: none
Storage Type: nonVolatile
Row Status: active
-----------------------------------------------
Engine ID: 80.00.08.1c.04.46.53
User: templateSHA
Authentication Protocol: SHA
Privacy Protocol: DES_CBC
Storage Type: nonVolatile
Row Status: active
-----------------------------------------------
```

Related Command(s)

- `snmp group` - Configures the SNMP group details
- `snmp user` - Configures the SNMP user details
- `show snmp community` - Displays the configured SNMP community details
- `snmp engineid` - Configures the engine identifier
- `snmp targetparams` - Configures the SNMP target parameters

show snmp notif

Command Objective This command displays the configured SNMP Notification types.

Syntax **show snmp notif**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp notif
Notify Name: smis
Notify Tag: smis
Notify Type: trap
Storage Type: volatile
Row Status: active
-----------------------------------------------
Notify Name: smis1
Notify Tag: smis1
Notify Type: trap
Storage Type: volatile
Row Status: active
```

Related Command(s)

- `snmp notify` - Configures the SNMP notification details
- `snmp targetparams` - Configures the SNMP target parameters
- `snmp-server trap udp-port`- Configures the udp port over which agent sends the trap

show snmp inform statistics

Command Objective This command displays the inform message statistics.

Syntax **show snmp inform statistics**

Mode Privileged EXEC Mode

Note: SNMP Manager must have been configured and Inform type notifications must have been generated.

Example

```
Your Product# show snmp inform statistics
Target Address Name : smismanager
IP Address          : 10.0.0.10
Inform messages sent : 20
Acknowledgement awaited for : 2 Inform messages
Inform messages dropped : 0
Acknowledgement failed for : 0 Inform messages
Informs retransmitted: 0
Inform responses received: 18
```

show snmp-server traps

Command Objective This command displays the set of traps that are currently enabled.

Syntax **show snmp-server traps**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp-server traps
Currently enabled traps:
--------------------------------------
linkup,linkdown,
```

Related Command(s) `snmp-server enable traps` - Enables generation of a particular trap.

show snmp-server proxy-udp-port

Command Objective This command displays the proxy udp port.

Syntax **show snmp-server proxy-udp-port**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp-server proxy-udp-port
snmp-server proxy-udp-port : 162
```

Related Command(s) `snmp-server trap proxy-udp-port` - Configures the udp port over which agent sends the trap.

show snmp tcp

Command Objective This command displays the configuration for snmp over tcp.

Syntax **show snmp tcp**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp tcp
snmp over tcp disabled
snmp trap over tcp disabled
snmp listen tcp port 161
Snmp listen tcp trap port 162
```

Related Command(s)

- `snmp tcp enable` – Enables sending snmp messages over tcp.
- `snmp trap tcp enable` - Enables sending snmp trap messages over tcp.
- `snmp-server tcp-ports` – Configures the tcp port over which agent sends the snmp message.
- `snmp-server trap tcp-ports` - Configures the tcp port over which agent sends the trap.

show snmp filter

Command Objective This command displays the configured SNMP filters.

Syntax **show snmp filter**

Mode Privileged EXEC Mode

Example

```
Your Product# show snmp filter
Filter Name : filter1
Subtree OID : 1.5
Subtree Mask : 1.1
Filter Type : Included
Storage Type : Non-volatile
Row Status  : Active
------------------------------------------------
```

Related Command(s) `snmp filterprofile` - Creates Notify filter Table

snmpset mib

Command Objective This command sets the value of the mib object through SNMP agent. This command is intended for internal testing purpose only

Syntax **snmpset mib {name | oid} <name/oid> value <string> [short] [<datatype - i, o, x, s>]**

Parameter Description

- `name <name>` - Sets the mib object name. This is a string value with maximum size as 32
- `oid <oid>` - Sets the mib object identifier. This is a string value with maximum size as 32.

- `value <string>` - Sets the value for the mib object.
- `short` - Displays the value of the mib object.
- `datatype` - Sets the specified datatype for the mib object.The data types are
  - `i` **–** Sets the integer value for the mibobject.
  - `s` - Sets the string value for the mib object.
  - `o` - Sets the Octet string value for the mib object.
  - `x` - Sets the hexa string value for the mib object.

Mode Global Configuration Mode

Example

```
Your Product (config)# snmpset mib name snmpListenTcpPort.0 value 145 short
1
```

Related Command(s)

- `show snmp` - Displays the status information of SNMP communications.
- `show mib name` – Displays the name of the corresponding Object Identifier.
- `show mib oid` - Displays the OID (Object Identifier) of the corresponding mib object.

snmpget mib

Command Objective This command gets the value of the mib object through SNMP agent. This command is intended for internal testing purpose only

Syntax **snmpget mib {name | oid} <value> [short]**

Parameter Description

- `name <value>` - Gets the mib object name. This is a string value with maximum size as 32.
- `oid <value>` - Gets the mib object identifier. This is a string value with maximum size as 32.
- `short` - Displays the value of the mib object.

Mode Global Configuration Mode

Example

```
Your Product (config)# snmpget mib name fsbgp4PeerExtConfigurePeer.12.0.0.1
short
```

Related Command(s)

- `show snmp` - Displays the status information of SNMP communications.
- `snmpset mib` - Sets the value of the mib object via SNMP agent.

snmpgetnext mib

Command Objective This command gets the next mib object for the given object. This command is intended for internal testing purpose only

Syntax **snmpgetnext mib {name | oid} <value> [short]**

Parameter Description

- name <value> - Gets the next mib object name. This is a string value with maximum size as 32.
- oid <value> - Gets the next mib object identifier. This is a string value with maximum size as 32.
- short - Displays the value of the mib object.

Mode Global Configuration Mode

Example

```
Your Product (config)# snmpgetnext mib name fsbgp4PeerExtTable short
```

Related Command(s) `show snmp` - Displays the status information of SNMP communications.

snmpwalk mib

Command Objective This command displays all the mib objects of the given table. This command is intended for internal testing purpose only

Syntax **snmpwalk mib {name | oid} <value> [count <integer(1-100)>] [short]**

Parameter Description

- **name <value>** - Gets the next mib object name for the given mib object name. This is a string value with maximum size as 32.
- **oid <value>** - Gets the next mib object identifier for the given mib object identifier.
- **count <integer(1-100)>** - Sets the number of entries to be displayed in the mib object. This value ranges between 1 and 100.
- **short** - Displays the value of the mib object.

Mode Global Configuration Mode

Example

```
Your Product (config)# snmpwalk mib name fsbgp4PeerExtTable
```

snmp filter trap

Command Objective This command sets the traps to be filtered.

The no form of the command removes the traps from filter table.

Syntax **snmp filter trap {name | oid} <name/oid>**

no snmp filter trap {name | oid} <name/oid>

Parameter Description

- `name <name>` - Gets the mib object name. This is a string value with maximum size as 32.

- `oid <oid>` - Gets the mib object identifier.

Mode Global Configuration Mode

Example

```
Your Product (config)# snmp filter trap name fsbgp4PeerExtTable
```

show mib oid

Command Objective This command displays the OID (Object Identifier) of the corresponding mib object name.

Note: This command is intended for internal testing purpose only

Syntax **show mib oid <object name. eg ifMainRowStatus>**

Mode Privileged EXEC Mode

Example

```
Your Product (config)# show mib oid fsbgp4PeerExtTable MIB OID for
fsbgp4PeerExtTable is 1.3.6.1.4.1.2076.41.2
```

Related Command(s) `snmpset mib` - Sets the value of the mib object via SNMP agent.

show mib name

Command Objective This command displays the name of the corresponding mib object identifier.

Note: This command is intended for internal testing purpose only

Syntax **show mib name <Object OID. eg 1.3.6.1.6>**

Mode Privileged EXEC Mode

Example

```
Your Product (config)# show mib name 1.3.6.1.4.1.2076.41.2 MIB Name for
1.3.6.1.4.1.2076.41.2 is fsbgp4PeerExtTable
```

Related Command(s) `snmpset mib` - Sets the value of the mib object via SNMP agent.

11 Syslog

Syslog is a protocol used for capturing log information for devices on a network. The syslog protocol provides a transport to allow a machine to send event notification messages across IP networks to event message collectors, also known as syslog servers. The protocol is simply designed to transport the event messages.

One of the fundamental tenets of the syslog protocol and process is its simplicity. The transmission of syslog messages may be started on a device without a receiver being configured, or even actually physically present. This simplicity has greatly aided the acceptance and deployment of syslog.

The list of CLI commands for the configuration of syslog is as follows:

- Logging
- logging synchronous
- mailserver
- sender mail-id
- cmdbuffs
- clear logs
- syslog mail
- syslog local storage
- syslog filename-one
- syslog filename-two
- syslog filename-three
- syslog relay - port
- syslog profile
- logging-file
- logging server
- syslog relay
- syslog relay transport type
- show logging
- show email alerts
- show syslog role
- show syslog mail
- show syslog localstorage
- show logging-file
- show logging-server
- show mail-server
- show syslog relay-port
- show syslog profile
- show syslog relay transport type
- show syslog file-name
- show syslog information
- smtp authentication
- snmp trap syslog-server-status

Logging

Command Objective This command enables syslog server and configures the syslog related parameters The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or syslog server.

The no form of the command disables syslog server and resets the configured parameters. The existing syslog buffers will not be cleared and none of the configured options will be changed, when the syslog feature is disabled.

Syntax **logging { buffered [<size (1-200)>] | console | facility {local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7|}| severity [{ <level (0-7)> | alerts | critical | debugging | emergencies | errors | informational | notification | warnings }] | on }**

no logging { buffered | console | facility | severity | on}

Parameter Description

- `buffered` - Limits Syslog messages displayed from an internal buffer. This size ranges between 1 and 200 entries.

  Note: The size feature is optional only in the code using the industrial standard command, otherwise this feature is mandatory.

- `console` - Limits messages logged to the console.
- `facility` - The facility that is indicated in the message. Can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, local7.
- `severity` - Message severity level. Messages with severity level equal to or high than the specified value are printed asynchronously. This can be configured using numerical value or using the available option. The options are:
    - `0 | emergencies` - System is unusable.
    - `1 | alerts` - Immediate action needed.
    - `2 | critical` - Critical conditions.
    - `3 | errors` - Error conditions.
    - `4 | warnings` - Warning conditions.
    - `5 | notification` - Normal but significant conditions.
    - `6 | informational` - Informational messages.
    - `7 | debugging`– Debugging messages.
- `alerts` - Immediate action needed
- `critical` - Critical conditions
- `debugging` - Debugging messages
- `emergencies` - System is unusable
- `errors` - Error conditions
- `informational` - Information messages
- `notification` - Normal but significant messages
- `warnings` - Warning conditions
- `on` - Syslog enabled

Mode Global Configuration Mode

Default

- console - enabled
- severity - informational, when no option is selected while configuration.

- debugging, at system start-up.
- buffered - 50
- facility - local0

  Note: The log file is stored in ASCII text format. The Privileged EXEC command is used to display its contents

- The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or Syslog server
- The existing syslog buffers will not be cleared and none of the configured options will be changed, when the Syslog feature is disabled

Example `Your Product (config)# logging buffered`

Related Command(s) `show logging` - Displays Logging status and configuration information

logging synchronous

Command Objective This command enables synchronous logging of messages. This command is a complete standardized implementation of the existing command. It operates similar to that of the command logging.

Syntax **logging synchronous {severity [{<short (0-7)> | alerts | critical | debugging | emergencies | errors | informational | notification | warnings|all}] | limit <number-of-buffers(size(1-200))}**

Parameter Description

- `severity` - Message severity level. Messages with severity level equal to or high than the specified value are printed asynchronously. This can be configured using numerical value or using the available option. The options are:
  - `0 | emergencies` - System is unusable.
  - `1 | alerts` - Immediate action needed.
  - `2 | critical` - Critical conditions.
  - `3 | errors` - Error conditions.
  - `4 | warnings` - Warning conditions.
  - `5 | notification` - Normal but significant conditions.
  - `6 | informational` - Informational messages.
  - `7 | debugging`– Debugging messages.
  - `all` - All messages are printed asynchronously regardless of the severity level.
- limit <number-of-buffers(size(1-200) - Number of buffers to be queued for the terminal after which new messages are dropped. This value ranges between 1 and 200 entries.

Mode Line Configuration Mode

Default

- severity - informational, when no option is selected while configuration. debugging, at system start-up.
- limit - 50

  Note: The log file is stored in ASCII text format. The Privileged EXEC command is used to display its contents.

- The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, logging file, or Syslog server.
- The existing syslog buffers will not be cleared and none of the configured options will be changed, when the Syslog feature is disabled.

Example

```
Your Product (config-line)# logging synchronous severity 4
```

Related Command(s) `show logging` - Displays Logging status and configuration information

mailserver

Command Objective This command sets the mail server IP address to be used for sending email alert messages.

The no form of the command re-sets the mail server IP address used for sending email alert messages.

Syntax **mail-server <short (0-191)> {ipv4 <ucast_addr> | ipv6 <ip6_addr> | <host-name>} <string(50)> [user <user_name> password <password>]**

no mail-server <short (0-191)> {ipv4 <ucast_addr> | ipv6 <ip6_addr> | <host-name>}

Parameter Description

- `<short (0-191)>` - Sets the priority for that particular mail-server configuration. The value ranges between 0 and 191.
- `ipv4<ucast_addr>` - Configures the ipv4 destination address for the syslog mail server
- `ipv6<ip6_addr>` - Configures the ipv6 destination address for the syslog mail server.
- <host-name> - Configures the host name for the syslog mail server.
- `<string(50)>` - Specifies the receiver mail id in which the email alert messages are received and logged.
- `user <user_name>` - Configures the user name of the account in the mail server to which the mails is to be sent. The user name is used only if a valid authentication method is configured for the system. The maximum allowed size in 64 characters.
- `password <password>` - Sets the password to authenticate the user name in the mail server.The password is used only if a valid authentication method is configured for the system. The maximum allowed size in 64 characters.

Mode Global Configuration Mode

Example `Your Product (config)# mail-server 190 ipv4 23.78.67.89 support@Aricent.com`

Related Command(s)

- `logging` - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
- `show email alerts` - Displays email alerts related configuration

sender mail-id

Command Objective This command sets the sender mail id from which the email alert messages are sent. The no form of the command deletes the configured sender mail id.

Syntax **sender mail-id <mail-id (100)>**

no sender mail-id

Mode Global Configuration Mode

Default syslog@supermicro.com

This command can be executed only if the mail server is configured.

Example `Your Product (config)# sender mail-id plabinik@supermicro.com`

Related Command(s)

- `mailserver` - Sets the mail server IP address to be used for sending email alert messages
- `logging` - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
- `show logging` - Displays Logging status and configuration information
- `show email alerts` - Displays email alerts related configuration
- `receiever mail-id` - Sets the receiver mail id

cmdbuffs

Command Objective This command configures the number of syslog buffers for a particular user. This command is not supported on some SMIS models.

Syntax **cmdbuffs <user name> <no.of buffers (1-200)>**

Parameter Description

- `<user name>` - User Name
- `<no.of buffers (1-200)>` - Number of log buffers to be allocated in the system

Mode Global Configuration Mode

Default 50

Example
```
Your Product(config)#cmdbuffs Aricent 50
```

Related Command(s)

- `logging` - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
- `show logging` - Displays Logging status and configuration information
- `clear logs` - Clears the logs buffered in the system.
- `username` - Creates a user and sets the enable password for that user with the privilege level.

clear logs

Command Objective This command clears the system syslog buffers.

Syntax **clear logs**

Mode Global Configuration Mode

Example
```
Your Product (config)# clear logs
```

Related Command(s)

- `cmdbuffs` - Configures the number of Syslog buffers for a particular user
- `logging` - Enables Syslog Server and configures the Syslog Server IP address, the log-level and other Syslog related parameter
- `show logging` - Displays Logging status and configuration information

syslog mail

Command Objective This command enables the syslog mail storage in the system. By enabling syslog mail storage, SMIS sends the syslog messages as mail messages to themail-server configured in the system. The no form of command disables the mail option in syslog.

Syntax **syslog mail**

no syslog mail

Mode Global Configuration Mode

Example
```
Your Product (config)# syslog mail
```

Related Command(s)

- `show syslog mail` - Displays the mail option in syslog.
- `mail server table` - Adds an entry to mail-server table.
- `show syslog information` - Displays the status of consolidated syslog log information.

syslog local storage

Command Objective This command enables the syslog file storage to log the status in the local storage path. The no form of command disables the syslog local storage.

Syntax **syslog localstorage**

no syslog localstorage

Mode Global Configuration Mode

Example

```
Your Product (config)# syslog localstorage
```

Related Command(s)

- `show syslog local storage` - Displays the syslog local storage.
- `syslog filename-one` - Configures the file name to store the syslog messages.
- `syslog filename-two` - Configures the file name to store the syslog messages.
- `syslog filename-three` - Configures the file name to store the syslog messages
- `logging-file` - Adds an entry in to file table
- `show syslog file-name` - Displays all the syslog local storage file names.
- `show syslog information` - Displays the status of consolidated syslog log information.

syslog filename-one

Command Objective This command configures a first file to store the syslog messages locally. The maximum size of the file name is 32.

Syntax **syslog filename-one <string(32)>**

Mode Global Configuration Mode

Note: This command is executed only if syslog local storage is enabled.

Example

```
Your Product (config)# syslog filename-one smis1
```

Related Command(s)

- `syslog local storage` - Enables the syslog local storage
- `logging-file` - Adds an entry in to file table
- `show syslog local storage` - Displays the syslog local storage.
- `show logging-file` - Displays the Syslog file table

- `show syslog file-name` - Displays all the syslog local storage file names.

syslog filename-two

Command Objective This command configures a second file name to store the syslog messages locally. The maximum size of the file name is 32.

Syntax **syslog filename-two <string(32)>**

Mode Global Configuration Mode

Note: This command is executed only if syslog local storage is enabled.

Example

```
Your Product (config)# syslog filename-two smis2
```

Related Command(s)

- `Syslog local storage` - Enables the syslog local storage
- `show syslog file-name` - Displays the Syslog local storage file name
- `logging-file` - Adds an entry in to file table
- `show syslog local storage` - Displays the syslog local storage.
- `show logging-file` - Displays the Syslog file table

syslog filename-three

Command Objective This command configures a third file name to store the syslog messages locally. The maximum size of the file name is 32.

Syntax **syslog filename-three <string(32)>**

Mode Global Configuration Mode

Note: This command is executed only if syslog local storage is enabled.

Example

```
Your Product (config)# syslog filename-three smis3
```

Related Command(s)

- `syslog local storage` - Enables the syslog local storage
- `show syslog file-name` - Displays the Syslog local storage file name
- `logging-file` - Adds an entry in to file table
- `show syslog local storage` - Displays the syslog local storage.
- `show logging-file` - Displays the Syslog file table

syslog relay - port

Command Objective This command sets the syslog port through which the relay receives the syslog messages irrespective of the transport type. The port number ranges between 0 and 65535.

The no form of command sets the syslog port to default port.

Syntax **syslog relay-port <integer(0-65535)>**

no syslog relay-port

Mode Global Configuration Mode

Default 514

Note: This command is executed only if syslog relay is enabled.

Example Your Product (config)# syslog relay-port 500

Related Command(s)

- `syslog relay` - Changes the syslog role from device to relay
- `syslog relay transport type` - Sets the syslog relay transport type either as udp or tcp
- `show syslog relay – port` - Displays the syslog relay port
- `show syslog relay transport type` - Displays the Syslog relay transport type

syslog profile

Command Objective This command sets the profile for reliable syslog.

The no form of command sets the profile to default (raw) for Reliable Syslog.

Syntax **syslog profile {raw | cooked}**

no syslog profile

Parameter Description

- `raw` - Sets the syslog profile as raw which is the profile for the transport type beep.
- `cooked` - Sets the syslog profile as cooked.

Note: This feature is not supported. It may be implemented in the future.

Mode Global Configuration Mode

Default Raw

Example

```
Your Product (config)# syslog profile raw
```

Related Command(s) `show syslog profile` - Displays the Syslog profile.

logging-file

Command Objective This command adds an entry in the file table.

The no form of command deletes an entry from the file table.

Syntax **logging-file <short(0-191)> <string(32)>**

no logging-file <short(0-191)><string(32)>

Parameter Description

- `<short(0-191)>` - Sets the priority of syslog messages. 0-lowest priority, 191-highest priority
- `<string(32)>` - Represents the file-name in which a log is done.

Mode Global Configuration Mode

Note: This command is executed only if local storage syslog is enabled.

Example

```
Your Product (config)# logging-file 134 smis1
```

Related Command(s)

- `show logging-file` - Displays the Syslog file table
- `syslog local storage` - Enables the syslog local storage
- `syslog file-one` - Configures the first file to store the syslog messages locally.
- `syslog filename-two` - Configures the second file name to store the syslog messages locally.

logging server

Command Objective This command configures a server table to log an entry in it. The no form of command deletes an entry from the server table.

Syntax **logging-server <short(0-191)> {ipv4 <ucast_addr> | ipv6 <ip6_addr> | <host-name>} [port <integer(0-65535)>] [{udp | tcp | beep}]**

no logging-server <short(0-191)> {ipv4 <ucast_addr> |ipv6 <ip6_addr> | <host-name>}

Parameter Description

- `<short(0-191)>` - Sets the priority for the syslog messages. 0-lowest priority, 191-highest priority.
- `ipv4 <ucast_addr>` - Sets the server address type as internet protocol version 4.
- `ipv6 <ip6_addr>` - Sets the server address type as internet protocol version 6.
- `<host-name>` - Configures the host name for a server to log an entry.
- `port<integer(0-65535)>` - Sets the port number through which it sends the syslog message. The value ranges between 0 and 65535.
- `udp` - Sets the forward transport type as udp.,

- `tcp` - Sets the forward transport type as tcp,
- `beep` - Sets the forward transport type as beep.

Mode Global Configuration Mode

Example

```
Your Product (config)# logging-server 134 ipv4 12.0.0.3
```

Related Command(s) `show logging-server` - Displays the Syslog logging server table

syslog relay

Command Objective This command changes the syslog role from device to relay.

The no form of command changes the syslog role from relay to device.

Syntax **syslog relay**

no syslog relay

Mode Global Configuration Mode

Example

```
Your Product (config)# syslog relay
```

Related Command(s)

- `show syslog relay-port` - Displays the syslog relay port
- `show syslog role` - Displays the syslog role.
- `syslog relay transport type` - Sets the syslog relay transport type either as udp or tcp
- `syslog relay – port` - Sets the syslog port through which it receives the syslog messages
- `show syslog relay transport type` - Displays the Syslog relay transport type
- `show syslog information` - Displays the status of consolidated syslog log information.

syslog relay transport type

Command Objective This command sets the Syslog relay transport type either as udp or tcp.

Syntax **syslog relay transport type {udp | tcp}**

Parameter Description

- `udp` - Sets the relay transport type as udp
- `tcp` - Sets the relay transport type as tcp

Mode Global Configuration Mode

Note: This command is executed only if syslog relay is enabled.

Example

```
Your Product (config)# syslog relay transport type udp
```

Related Command(s)

- `syslog relay` - Changes the syslog role from device to relay
- `show syslog role` - Displays the syslog role.
- `syslog relay`- port - Sets the syslog port through which it receives the syslog messages
- `show syslog relay transport type` - Displays the Syslog relay transport type
- `show syslog relay - port` - Displays the Syslog relay port.

show logging

Command Objective This command displays all the logging status and configuration information.

Syntax **show logging**

Mode Privileged EXEC Mode

Example

```
Your Product# show logging
System Log Information
-----------------------------------
Syslog logging              : enabled(Number of messages 0)
Console logging             : enabled(Number of messages 1) TimeStamp option
: enabled
Severity logging            : Debugging
Log server IP        : 10.0.0.1
Facility             : Default (local0)
Buffered size        : 100 Entries
LogBuffer(0 Entries, 0 bytes)
<129>Aug 7 12:08:02 ISS CLI Attempt to login as root via console Succeeded
```

Related Command(s)

- `logging` - Enables Syslog Server and configures Syslog Server IP address, log-level and other Syslog related parameter
- `sender mail-id` - Sets the sender mail id from which the email alert messages are sent.
- `cmdbuffs` - Configures the number of syslog buffers for a particular user.
- `clear logs` - Clears the logs buffered in the system.

show email alerts

Command Objective This command displays configurations related to email alerts.

Syntax **show email alerts**

Mode Privileged EXEC Mode

Note: This command is executed only if mail server is configured.

Example

```
            Your Product# show email alerts
            Sender email-id   : plabinik@Aricent.com
```

Related Command(s)

- `mail-server` - Sets the mail server IP address to be used for sending email alert messages
- `sender mail-id` - Sets the sender mail id from which the email alert messages are sent.

show syslog role

Command Objective This command displays the syslog role.

Syntax **show syslog role**

Mode Privileged EXEC Mode

Example

```
Your Product# show syslog role
Syslog Role    : Relay
```

Related Command(s)

- `syslog relay` - Changes the syslog role from device to relay
- `syslog relay transport type` - Sets the syslog relay transport type either as udp or tcp

show syslog mail

Command Objective This command displays status of the mail option in syslog.

Syntax **show syslog mail**

Mode Privileged EXEC Mode

Example

```
            Your Product# show syslog mail
            Syslog Mail Option    : Enabled
```

Related Command(s) `syslog mail` – Enables the mail option in syslog

show syslog localstorage

Command Objective This command displays the syslog local storage.

Syntax **show syslog localstorage**

Mode Privileged EXEC Mode

Example

```
Your Product# show syslog localstorage
Syslog Localstorage : Enabled
```

Related Command(s)

- `syslog local storage` - Enables the syslog local storage
- `syslog filename`-one - Configures the first file to store the syslog messages locally
- `syslog filename-two` - Configures the second file name to store the syslog messages locally
- `syslog filename-three`- Configures the third file name to store the syslog messages locally
- `shpw syslog file-name` - Displays all the syslog local storage file names.

show logging-file

Command Objective This command displays the priority and file name of all the three files configured in the syslog file table.

Syntax **show logging-file**

Mode Privileged EXEC Mode

Example

```
Your Product# show logging-file
Syslog File Table Information
---------------------------------------------
Priority        File-Name
------------    ---------------------
134             smis1
134             smis2
134             smis3
```

Related Command(s)

- `syslog` - Configures the first file to store the syslog messages locally
- `syslog filename-two` - Configures the second file name to store the syslog messages locally
- `syslog filename-three`- Configures the third file name to store the syslog messages locally
- `logging-file` - Adds an entry in to file table

show logging-server

Command Objective This command displays the information about the syslog logging server table.

Syntax **show logging-server**

Mode Privileged EXEC Mode

Example

```
Your Product# show logging-server
Syslog Forward Table Information
------------------------------------------------------------
Priority      Address-Type  IpAddress     Port   Trans-Type
------------  --------------------------  ------------------------------------------------
129           ipv4          12.0.0.2      514    udp
134           ipv4          12.0.0.1      514    udp
```

Related Command(s) `logging server` - Adds an entry in to logging-server table

show mail-server

Command Objective This command displays the information about the syslog mail server table.

Syntax **show mail-server**

Mode Privileged EXEC Mode

Example

```
Your Product# show mail-server
Syslog Mail Table Information
-------------------------------------------------------------
Priority      Address-Type  IpAddress     Receiver Mail-Id UserName
--------------  --------------------------  -------------------  --------------------------
3             ipv4          23.78.67.89   support1@supermicro.com
13            ipv4          23.78.67.89   support1@supermicro.com
190           ipv4          23.78.67.89   support@supermicro.com
```

Related Command(s) `mail server table` - Adds an entry to mail-server table

show syslog relay-port

Command Objective This command displays the Syslog relay port.

Syntax **show syslog relay-port**

Mode Privileged EXEC Mode

Example

```
Your Product# show syslog relay-port

Syslog Port   : 251
```

Related Command(s)

- `syslog relay – port` - Sets the syslog port through which it receives the syslog messages

- `syslog relay` - Changes the syslog role from device to relay
- `syslog relay transport type` - Sets the syslog relay transport type either as udp or tcp

show syslog profile

Command Objective This command displays the syslog profile.

Syntax **show syslog profile**

Mode Privileged EXEC Mode

Example

```
Your Product# show syslog profile

Syslog Profile       : raw
```

Related Command(s) `syslog profile` - Sets the profile for reliable syslog

show syslog relay transport type

Command Objective This command displays the Syslog relay transport type.

Syntax **show syslog relay transport type**

Mode Privileged EXEC Mode

Example

```
Your Product# show syslog relay transport type

Syslog Relay Transport type udp
```

Related Command(s)

- `syslog relay transport type` - Sets the Syslog relay transport type either as udp or tcp
- `syslog relay -port` - Sets the syslog port through which it receives the syslog messages
- `syslog relay` - Changes the syslog role from device to relay

show syslog file-name

Command Objective This command displays all the syslog local storage file names.

Syntax **show syslog file-name**

Mode Privileged EXEC Mode

Example

```
Your Product# show syslog file-name
Syslog File Name
----------------------------------- Syslog File-One :smis1
Syslog File-Two :smis2
Syslog File-Three :smis3
```

Related Command(s)

- `syslog local storage` - Enables the syslog local storage
- `show syslog local storage` - Displays the syslog local storage.
- `syslog filename-one` - Configures the file name to store the syslog messages.
- `syslog filename-two` - Configures the file name to store the syslog messages.
- `syslog filename-three` - Configures the file name to store the syslog messages

show syslog information

Command Objective This command displays the status of consolidated syslog log information.

Syntax **show syslog information**

Mode Privileged EXEC Mode

Example

```
Your Product# show syslog information

System Log Information
----------------------------------
Syslog Localstorage    : Enabled
Syslog Mail Option    : Enabled
Syslog Port    : 251
Syslog Role    : Relay
Smtp Authentication   : None
```

Related Command(s)

- `syslog local storage` - Enables the syslog local storage
- `syslog mail` – Enables the mail option in syslog
- `syslog relay` - Changes the syslog role from device to relay
- `smtp authentication` - Sets the smtp authentication method while sending E-mail alerts to the mail server configured

smtp authentication

Command Objective This command sets the smtp authentication method while sending E-mail alerts to the mail server configured.

The no form of the command resets the authentication method to send email alerts with any authentication

Syntax **smtp authentication {auth-login | auth-plain | cram-md5 | digest-md5}**

no smtp authentication

Parameter Description

- `auth-login` - Sets the smtp authentication method as auth-login in which both the user name and password are BASE64 encoded
- `auth-plain` - Sets the smtp authentication method as auth-plain in which the user name and password used for authentication are combined to one string and BASE64 encoded.
- `cram-md5` - Sends the BASE64 encoded user name and 16-byte digest in hexadecimal notation. The digest is generated using HMAC calculation with password as secret key and SMTP server original challenge as the message.
- `digest-md5` - Sets the smtp authentication method as digest-md5 in which the BASE64 encoded MD5 digest response string that is calculated using the user name, password, realm string and nonce string.

Mode Global Configuration Mode

Example `Your Product (config)# smtp authentication auth-login`

Related Command(s) `show syslog information` - Displays the status of consolidated syslog log information

snmp trap syslog-server-status

Command Objective This command enables trap generation when the syslog server is down.

The no form of the command disables trap generation when the syslog server is down

Syntax **snmp trap syslog-server-status**

no snmp trap syslog-server-status

Parameter Description

- `trap` - Configures trap related parameters.
- `syslog-server-status` - Configures syslog server related configurations.

Mode Global Configuration Mode

Default Syslog server trap generation is enabled

Example `Your Product (config)# snmp trap syslog-server-status`

12 TCP

Transmission Control Protocol (TCP) is an implementation of the industry standard TCP based on RFC 793. The software consists of the core TCP protocol, a library that provides a Socket Layer Interface to support both Telnet Server and HTTP server. TCP interacts with the Network Layer protocols (IPv4/IPv6) and uses their services for end-to-endcommunication.

The list of TCP commands is as follows:

- show tcp statistics
- show tcp connections
- show tcp listeners
- show tcp retransmission details
- tcp max retries

show tcp statistics

Command Objective This command displays the tcp statistics information such as Max connections, Active opens, Passive opens and attempts fail.

Syntax **show tcp statistics [vrf <vrf-name>]**

Parameter Description `vrf <vrf-name>` - Displays the tcp statistics information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Note: Settings can be configured for the specified VRF through SNMP and when no VRF instance is mentioned the settings are configured for the default VRF.

Mode Privileged EXEC Mode

Example

```
Your Product# show tcp statistics
Context Name : default
Max Connections : 500
Active Opens : 0
Passive Opens : 0
Attempts Fail : 0
           Estab Resets : 0
Current Estab : 0
Input Segments : 0
Output Segments : 0
Retransmitted Segments : 0
Input Errors : 0
TCP Segments with RST flag Set: 0
HC Input Segments : 0
HC Output Segments : 0
```

```
Context Name : vrf1
Max Connections : 500
Active Opens : 0
Passive Opens : 0
Attempts Fail : 0
Estab Resets : 0
Current Estab : 0
Input Segments : 0
Output Segments : 0
Retransmitted Segments : 0
Input Errors : 0
TCP Segments with RST flag Set: 0
HC Input Segments : 0
HC Output Segments : 0
Context Name : vrf2
```

```
Max Connections : 500
Active Opens : 0
Passive Opens : 0
Attempts Fail : 0
Estab Resets : 0
Current Estab : 0
Input Segments : 0
Output Segments : 0
Retransmitted Segments : 0
Input Errors : 0
TCP Segments with RST flag Set: 0
HC Input Segments : 0
HC Output Segments : 0
Context Name : vrf3
Max Connections : 500
Active Opens : 0
Passive Opens : 0
Attempts Fail : 0
Estab Resets : 0
Current Estab : 0
Input Segments : 0
Output Segments : 0
Retransmitted Segments : 0
Input Errors : 0
TCP Segments with RST flag Set:   0
HC Input Segments : 0
HC Output Segments : 0
Context Name : vrf4
Max Connections : 500
Active Opens : 0
Passive Opens : 0
Attempts Fail : 0
Estab Resets : 0
Current Estab : 0
Input Segments : 0
Output Segments : 0
Retransmitted Segments : 0
Input Errors : 0
TCP Segments with RST flag Set: 0
HC Input Segments : 0
HC Output Segments : 0
Your Product# show tcp statistics vrf vrf1
Context Name : vrf1
Max Connections : 500
Active Opens : 0
Passive Opens : 0
Attempts Fail : 0
Estab Resets : 0
Current Estab : 0
Input Segments : 0
Output Segments : 0
Retransmitted Segments : 0
Input Errors : 0
TCP Segments with RST flag Set: 0
HC Input Segments : 0
HC Output Segments : 0
```

show tcp connections

Command Objective This command displays the tcp connections for the switch such as Local IP Address type, Local IP, Local Port and Remote Port. It also displays if a connection is TCP MD5 protected and the number of incoming segments that failed MD5 authentication.

Syntax **show tcp connections [vrf <vrf-name>]**

Parameter Description `vrf <vrf-name>` - Displays the tcp connections for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32

Note: Connections can be configured for the specified VRF through SNMP and when no VRF instance is mentioned the settings are configured for the default VRF

Mode Privileged EXEC Mode

Example

```
Your Product# show tcp connections
Context Name : default

TCP Connections
===============

Local IP Address Type : IPv4
Local IP              : 0.0.0.0
Local Port            : 22
Remote IP Address Type : IPv4
Remote IP             : 0.0.0.0
Remote Port           : 0
TCP State             : Listen
MD5 Authenticated     : No

TCP Connections
===============

Local IP Address Type : IPv4
Local IP              : 0.0.0.0
Local Port            : 23
Remote IP Address Type : IPv4
Remote IP             : 0.0.0.0
Remote Port           : 0
TCP State             : Listen
MD5 Authenticated     : No

TCP Connections
===============

Local IP Address Type : IPv4
Local IP              : 0.0.0.0
Local Port            : 80
```

```
Remote IP Address Type : IPv4
Remote IP              : 0.0.0.0
Remote Port            : 0
TCP State              : Listen
MD5 Authenticated      : No
TCP Connections
===============

Local IP Address Type : IPv4
Local IP              : 0.0.0.0
Local Port            : 646
Remote IP Address Type : IPv4
Remote IP              : 0.0.0.0
Remote Port            : 0
TCP State              : Listen
MD5 Authenticated      : No

TCP Connections
===============

Local IP Address Type : IPv6
Local IP              : :: Local Port           : 22
Remote IP Address Type : IPv6
Remote IP              : :: Remote Port          : 0
TCP State              : Listen
MD5 Authenticated      : No

TCP Connections
===============

Local IP Address Type : IPv6
Local IP              : :: Local Port           : 23
Remote IP Address Type : IPv6
Remote IP              : :: Remote Port          : 0
TCP State              : Listen
MD5 Authenticated      : No

TCP Connections
===============

Local IP Address Type : IPv6
Local IP              : :: Local Port           : 80
Remote IP Address Type : IPv6
Remote IP              : :: Remote Port          : 0
TCP State              : Listen
MD5 Authenticated      : No
Context Name : vrf1
Context Name : vrf2
Context Name : vrf3
Context Name : vrf4
```

show tcp listeners

Command Objective This command displays the information such as Local IP Address Type, Local IP and

Local Port for each listeners in the network.

Syntax **show tcp listeners [vrf <vrf-name>]**

Parameter Description `vrf <vrf-name>` - Displays the TCP listener information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Note: Settings can be configured for the specified VRF through SNMP and when no VRF instance is mentioned the settings are configured for the default VRF.

Mode Privileged EXEC Mode

Example

```
Your Product# show tcp listeners
Context Name : default

TCP Listeners
===============

Local IP Address Type : 0
Local IP              : 0.0.0.0
Local Port            : 22
Local IP Address Type : 0
Local IP              : 0.0.0.0
Local Port            : 23
Local IP Address Type : 0
Local IP              : 0.0.0.0
Local Port            : 80
Address Type [0 - IPv4 and IPv6] [1 - IPv4] [2 - IPv6] Context Name : vrf1
Context Name : vrf2
Context Name : vrf3
Context Name : vrf4
Your Product# show tcp listeners vrf default
Context Name : default

TCP Listeners
===============
Local IP Address Type : 0
Local IP              : 0.0.0.0
Local Port            : 22
Local IP Address Type : 0
Local IP              : 0.0.0.0
Local Port            : 23
Local IP Address Type : 0
Local IP              : 0.0.0.0
Local Port            : 80
Address Type [0 - IPv4 and IPv6] [1 - IPv4] [2 - IPv6]
```

show tcp retransmission details

Command Objective This command displays the tcp retransmission details.

Syntax **show tcp retransmission details [vrf <vrf-name>]**

Parameter Description `vrf <vrf-name>` - Displays the TCP transmission details for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Note: The retransmission settings can be configured for the specified VRF through SNMP and when no VRF instance is mentioned the settings are configured for the default VRF.

Mode Privileged EXEC Mode

Example

```
Your Product# show tcp retransmission details
Context Name : default
RTO Algorithm Used : VAN JACOBSON Min Retransmission Timeout : 0 msec Max
Retransmission Timeout : 0 msec
Context Name : vrf1
RTO Algorithm Used : VAN JACOBSON Min Retransmission Timeout : 0 msec Max
Retransmission Timeout : 0 msec
Context Name : vrf2
RTO Algorithm Used : VAN JACOBSON Min Retransmission Timeout : 0 msec Max
Retransmission Timeout : 0 msec
Context Name : vrf3
RTO Algorithm Used : VAN JACOBSON Min Retransmission Timeout : 0 msec Max
Retransmission Timeout : 0 msec
Context Name : vrf4
RTO Algorithm Used : VAN JACOBSON Min Retransmission Timeout : 0 msec Max
Retransmission Timeout : 0 msec
Your Product# show tcp retransmission details vrf default
Context Name : default
RTO Algorithm Used : VAN JACOBSON Min Retransmission Timeout : 0 msec Max
Retransmission Timeout : 0 msec
```

tcp max retries

Command Objective This command configures the maximum number of retries for re-transmission in TCP module.

Syntax **tcp max retries {<integer(1-12)>} [vrf <vrf-name>]**

Parameter Description

- `<integer(1-12)>` - Configures the maximum number of retries done by TCP module. This value ranges between 1 and 12.
- `vrf <vrf-name>`- Configures the maximum number of retries for re- transmission for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Note: When no VRF instance is mentioned the max retries is configured for the default VRF

Mode Global Configuration Mode

Example

```
Your Product (config)# tcp max retries 1
```

13 UDP

Aricent UDP (User Datagram Protocol) is an implementation of the industry standard UDP. It is used in packet-switched computer communication networks and in interconnected systems of such networks.

The software consists of the core UDP protocol and a library that provides a Socket Layer Interface for applications like SNMP. It supports a number of standard features in addition to the core protocol.
The following are the list of UDP commands:

- `show udp statistics`
- `show udp connections`

show udp statistics

Command Objective This command displays the udp statistics such as InDatagrams, outDatagrams, HC InDatagrams, HC OutDatagrams, UDP No Ports and UDP IN Errors. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Syntax **show udp statistics [vrf <vrf-name>]**

Mode Privileged EXEC Mode

Default vrf - default

Example

```
Your Product# show udp statistics vrf vr1

Global UDP Statistics
=========================
InDatagrams             : 0
OutDatagrams            : 0
HC InDatagrams          : 0
HC OutDatagrams         : 0
UDP No Ports            : 4
UDP In Errors           : 0
UDP with no Checksum    : 0
No. ICMP error packets  : 0
UDP with wrong Checksum  : 0
UDP In Broadcast Mode   : 0
Virtual Context - UDP Statistics
==================================
VRF  Name: vr1
-----------------
```

```
InDatagrams             :  0
OutDatagrams            :  0
HC InDatagrams          : 0
HC OutDatagrams         : 0
UDP No Ports            : 0
UDP In Errors           : 0
UDP with no Checksum    : 0
No. ICMP error packets : 0
UDP with wrong Checksum : 0
UDP In Broadcast Mode   : 0
```

Related Command(s) `show udp connections` – Displays the udp configurations for different connections.

show udp connections

Command Objective This command displays the udp configurations such as Local IP Address Type, Local IP, Local Port, Remote IP Address Type, Remote IP and Remote Port for various connections.

Syntax **show udp connections [vrf <vrf-name>]**

Parameter Description `vrf <vrf-name>` - Displays UDP information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Privileged EXEC Mode

Example

```
Your Product# show udp connections
Global UDP Connections
========================
Local IP Address Type : 0
Local IP              : 0.0.0.0
Local Port            : 161
Remote IP Address Type : 0
Remote IP             : 0.0.0.0
Remote Port           : 0
Local IP Address Type : 0
Local IP              : 0.0.0.0
Local Port            : 6125
Remote IP Address Type : 0
Remote IP             : 0.0.0.0
Remote Port           : 0
Local IP Address Type : 0
Local IP              : 0.0.0.0
Local Port            : 49152
Remote IP Address Type : 0
Remote IP             : 0.0.0.0
Remote Port           : 0
```

Related Command(s) `show udp statistics` – Displays the udp statistics.

14 L2 DHCP Snooping

The DHCP snooping feature filters the untrusted DHCP messages and builds a DHCP snooping binding database. It acts as a firewall between untrusted hosts and DHCP servers. These untrusted messages are sent from devices outside a network and are usually sources of traffic attacks. DHCP snooping binding database maintains a table which contains MAC address, IP address, lease time, binding type, VLAN number and interface information of the local untrusted interfaces of the switch.

The switch uses DHCP option 82 information, relay agent information, to establish the binding datatbase. DHCP server has to support this option and client has to disable this option for the proper operation of DHCP snooping.

The list of CLI commands used to configure the L2 DHCP snooping are:

- ip dhcp snooping - Global Command
- ip dhcp snooping verify mac-address
- ip dhcp snooping - VLAN Interface Command
- ip dhcp snooping trust
- show ip dhcp snooping globals
- show ip dhcp snooping vlan
- debug ip dhcp snooping

ip dhcp snooping - Global Command

Command Objective This command globally enables the layer 2 DHCP snooping in the switch or enables the snooping in the specific VLAN. The DHCP snooping module will start the protocol operation when the snooping is enabled globally. This value ranges between 1 and 4094. This is a unique value that represents the specific VLAN created.

The no form of the command globally disables layer 2 DHCP snooping in the switch or disables DHCP snooping in the specific VLAN. The DHCP snooping module will stop the protocol operation when the snooping is globally disabled.

Syntax **ip dhcp snooping [vlan < vlan-id (1-4094)>]**

no ip dhcp snooping [vlan <integer(1-4094)>]

Mode Global Configuration mode

Default DHCP snooping is globally disabled in the switch and on all VLAN's.

The Example used and the ip dhcp snooping command used in the config-vlan mode serve the same purpose.

Example

```
Your Product (config)# ip dhcp snooping vlan 2
```

Related Command(s)

- `show ip dhcp snooping globals` – Displays the global configuration of dhcp snooping
- `show ip dhcp snooping vlan` – Displays the configuration and statistics of the specified VLAN

ip dhcp snooping verify mac-address

Command Objective This command globally enables DHCP MAC verification in the switch.

The no form of the command globally disables DHCP MAC verification in the switch.

If the MAC verification status is enabled, DHCP snooping module will verify whether the source Mac address and client hardware Mac address are same. If they are same, packet will be processed further, else, it is dropped.

Syntax **ip dhcp snooping verify mac-address**

no ip dhcp snooping verify mac-address

Mode Global Configuration Mode

Default DHCP MAC address verification is enabled.

Example

```
Your Product (config)# ip dhcp snooping verify mac-address
```

Related Command(s) `show ip dhcp snooping globals` - Displays the global configuration of dhcp snooping

ip dhcp snooping - VLAN Interface Command

Command Objective This command enables layer 2 DHCP snooping in the VLAN.

The no form of the command disables layer 2 DHCP snooping in the VLAN. DHCP snooping feature filters the untrusted DHCP messages to provide security for DHCP servers.

Syntax **ip dhcp snooping**

no ip dhcp snooping

Mode Config-VLAN mode

Default L2 DHCP snooping is disabled on VLANs

Example

```
Your Product (config-vlan)# ip dhcp snooping
```

Related Command(s)

- `show ip dhcp snooping vlan` - displays the configuration and statistics of the specified VLAN
- `ip dhcp snooping` – Global command – This command enables layer 2 dhcp snooping on a particular VLAN.

ip dhcp snooping trust

Command Objective This command configures the port as a trusted port.

The no form of the command configures the port as an untrusted port.

The packets coming from the trusted port is considered as trusted packets and are not filtered by the DHCP snooping feature.

Syntax **ip dhcp snooping trust**

no ip dhcp snooping trust

Mode Interface Configuration mode

Default Ports are considered as trusted

Example

```
Your Product (config-if)# ip dhcp snooping trust
```

show ip dhcp snooping globals

Command Objective This command displays the global configuration of DHCP snooping. The global status of layer 2 DHCP snooping and MAC verification are displayed.

Syntax **show ip dhcp snooping globals [switch <Context Name>]**

Parameter Description `switch<Context Name>` - Displays the global configuration of DHCP snooping for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to MI feature.

Mode Privileged EXEC mode

Example

```
Your Product# show ip dhcp snooping globals

DHCP Snooping Global information
--------------------------------------------------------------------------------------

Layer 2 DHCP Snooping is globally disabled

MAC Address verification is enabled
```

Related Command(s)

- `ip dhcp snooping` – Global command - Globally enables the layer 2 DHCP snooping in the switch and allocates the resources for the DHCP snooping module.

- `ip dhcp snooping verify mac-address` – Globally enables DHCP MAC verification in the switch.

show ip dhcp snooping vlan

Command Objective This command displays the DHCP snooping configuration and statistics of all VLANs in which the DHCP snooping feature is enabled.

Syntax **show ip dhcp snooping [vlan <vlan-id (1-4094)>] [switch <context name>]**

Parameter Description

- `vlan <vlan-id (1-4094)>` - Displays the DHCP snooping configuration and statistics for the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
- `switch<context name>` - Displays the DHCP snooping configuration and statistics for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to MI feature.

Mode Privileged EXEC mode

Example

```
Your Product# show ip dhcp snooping vlan 3
DHCP Snooping Vlan information
-----------------------------------------------------------------
VLAN                              : 3
Snooping status                   : Enabled
Number of Incoming Discovers      : 0
Number of Incoming Requests       : 0
Number of Incoming Releases       : 0
Number of Incoming Declines       : 0
Number of Incoming Informs        : 0
Number of Transmitted Offers      : 0
Number of Transmitted Acks        : 0
Number of Transmitted Naks        : 0
Total Number Of Discards          : 0
Number of MAC Discards            : 0
Number of Server Discards         : 0
Number of Option Discards         : 0
```

Related Command(s) `ip dhcp snooping` - VLAN interface command - Enables layer 2 DHCP snooping in the VLAN.

debug ip dhcp snooping

Command Objective This command enables the tracing of the DHCP snooping module as per the configured debug level. The trace statements are generated for the configured trace levels.

The no form of the command disables the tracing of the DHCP module. The trace statements are not generated for the configured trace levels.

This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

Syntax **debug ip dhcp snooping {[entry][exit][debug][fail] | all}**

no debug ip dhcp snooping

Parameter Description

- `entry` - Generates debug statements for function entry traces. The names of the functions entered are displayed in the log.
- `exit` - Generates debug statements for function exit traces. The names of the functions exited are displayed in the log.
- `debug` – Generates debug statements for debug traces. This is used for debugging the packet flow of DHCP snooping functionality.
- `fail` - Generates debug statements for all failure traces. These traces are used for all valid and invalid failures. The valid failures represent the expected error. The invalid failures represent the unexpected error.
- `all` - Generates debug statements for all types of traces .

Mode Privileged EXEC mode

Example

```
Your Product# debug ip dhcp snooping entry
```

15 IPDB

IP source guard is used to restrict the IP traffic on Layer 2 interfaces by filtering traffic based on the IP binding database.

The list of CLI commands for the configuration of IPDB is as follows:

- ip binding
- ip source binding
- ip verify source
- show ip binding
- show ip source binding
- show ip binding counters
- show ip verify source
- debug ip binding database

ip binding

Command Objective This command configures the static binding information for the hosts connected to the switch.

The no form of the command deletes the binding information for the specified host.

Syntax **ip binding <mac-address> vlan <vlan-id (1-4094)> <ip address> interface <interface-type> <interface-id> gateway <ip address>**

no ip binding <mac-address> vlan <vlan-id (1-4094)>

Parameter Description

- `<mac-address>` - Configures the unicast MAC address of the host for which the binding information should be configured.
- `<vlan-id (1-4094)>` - Configures the VLAN ID to which the host belongs. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
- `<ip address>` - Configures IP address of the host for which the binding information should be configured.
- `<interface-type>` - Configures the type of interface to which the host is connected. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Configures the interface identifier to which the host is connected. This is a unique value that represents the specific interface.

  This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.

- `gateway <ip address>`- Configures the IP address of the gateways to which the host has access.

Mode Global Configuration mode

Example

```
Your Product (config)# ip binding 00:01:02:03:04:05 vlan 3 30.0.0.4
interface gigabitethernet 0/2 gateway 30.0.0.1
```

Related Command(s)

- `show ip binding` - Displays the IP binding database.
- `show ip binding counters` - Displays the global or VLAN statistics information.

ip source binding

Command Objective This command adds a static IP source binding entry.

The no form of the command deletes the static IP source binding entry.

Syntax **ip source binding <mac-address> vlan <vlan-id (1-4094)> <ip-address> interface <interface-type> <interface-id> [gateway <gateway-ip>]**

no ip source binding <mac-address> vlan <vlan-id (1-4094)> <ip-address> interface <interface-type> <interface-id>

Parameter Description

- `<mac-address>` - Configures the unicast MAC address of the host for which the binding information should be configured.
- `<vlan-id (1-4094)>` - Configures the VLAN ID to which the host belongs. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
- `<ip-address>` - Configures IP address of the host for which the binding information should be configured.
- `<interface-type>` - Configures the type of interface to which the host is connected. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Configures the interface identifier to which the host is connected. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.
- `gateway <gateway-ip>` - Configures the gateway IP address of the gateways to which the host has access.

Mode Global Configuration mode

Example

```
Your Product (config)# ip source binding 00:01:02:03:04:05 vlan 3 30.0.0.4
```

```
interface gigabitethernet 0/2 gateway 30.0.0.1
```

Related Command(s) `ip source binding` - Displays the source IP binding database.

ip verify source

Command Objective This command enables the IP source guard status for the specified interface.

The no form of the command disables the IP source guard on an interface.

The port-security option is mandatory for this command. Else the following error message gets displayed 'IP source guard feature does not support source IP filter type.

Syntax **ip verify source [port-security]**

no ip verify source [port-security]

Mode Interface Configuration Mode

Default Disable

Example

```
Your Product (config-if)# ip verify source port-security
```

Related Command(s) `show ip verify source` – Displays the IP source guard interface status.

show ip binding

Command Objective This command displays the IP binding database.

Syntax **show ip binding [vlan <vlan-id (1-4094)>] {[static | dhcp| ppp]} [switch <switch_name>]**

Parameter Description

- `vlan <vlan-id (1-4094)>` - Displays the VLAN ID to which the host belongs. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
- `static` - Displays the static ip binding configuration.
- `dhcp` - Displays the dynamic IP binding updates through DHCP snooping.
- `ppp` - Displays the dynamic IP binding updates through Pppoe intermediate agent.
- `switch <switch_name>` - Displays the database of the specified switch.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip binding vlan 2 static

Host Binding Information
-------------------------------------
VLAN HostMac           HostIP    Port   GatewayIP Type
------- ------------------------ ------------  ------- ---------------- --------
-
```

```
2    00:10:12:13:13:15 12.0.0.1 Gi0/1  12.0.0.0 static
```

Related Command(s) `ip binding` – Configures the static binding information for the hosts connected to the switch.

show ip source binding

Command Objective This Command displays the source IP binding database.

Syntax **show ip source binding [<ip-address>] [<mac-address>] [{ dhcp-snooping | static }] [interface <interface-type> <interface-id>] [vlan <vlan-id (1-4094)>] [switch <switch_name>]**

Parameter Description

- `<ip-address>` - Displays the IP address of the host for which the binding information should be configured.
- `<mac-address>` - Displays the unicast MAC address of the host for which the binding information should be configured.
- `dhcp-snooping` - Displays the dynamic IP binding updation through DHCP snooping.
- `static` - Displays the static ip binding configuration.
- `<interface-type>` - Displays the type of interface to which the host is connected. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Displays the interface identifier to which the host is connected. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.
- `vlan <vlan-id (1-4094)>` - Displays the VLAN ID to which the host belongs. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
- `switch <switch_name>` - Displays the status of the ip source binding of the specified switch.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip source binding
Host Binding Information
------------------------------------
```

```
VLAN    HostMac      HostIP     Port      GatewayIP Type
-------- -------------------- --------------- ---------------- -------------------- --------
-
```

Related Command(s) `ip source binding` - Adds a static IP source binding entry

show ip binding counters

Command Objective This command displays the global or VLAN statistics information.

Syntax **show ip binding counters [{[vlan <short (1-4094)>] | global | [switch <switch-name>] }]**

Parameter Description

- `vlan <short (1-4094)`> - Displays the VLAN ID to which the host belongs. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
- `global` - Displays the static information of all binding types (static, dhcp, ppp)
- `switch <switch-name>` - Displays the static information of the specified VLAN.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip binding counters vlan 2
Global Binding count Information
-------------------------------------------------- Number of Bindings        : 1
Number of Static Bindings : 1
Number of DHCP Bindings   : 0
Number of PPP Bindings    : 0
```

Related Command(s) `ip binding`- Configures the static binding information for the hosts connected to the switch.

show ip verify source

Command Objective This command displays the IP source guard interface status.

Syntax **show ip verify source [interface <interface-type> <interface-id>]**

Parameter Description

- `<interface-type>` - Displays the type of interface to which the host is connected. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.

- `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.

- `<interface-id>` - Configures the interface identifier to which the host is connected. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip verify source
Interface            IP Source guard Status
---------------      -----------------------------------
Gi0/1                Disable
Gi0/2                Disable
Gi0/3                Disable
Gi0/4                Disable
Gi0/5                Disable
Gi0/6                Disable
Gi0/7                Disable
Gi0/8                Disable
Gi0/9                Disable
Gi0/10               Disable
Gi0/11               Disable
Gi0/12               Disable
Gi0/13               Disable
Gi0/14               Disable
Gi0/15               Disable
Gi0/16               Disable
Gi0/17               Disable
Gi0/18               Disable
Gi0/19               Disable
Gi0/20               Disable
Gi0/21               Disable
Gi0/22               Disable
Gi0/23               Disable
Gi0/24               Disable
```

Related Command(s) `ip verify source` - Enables the IP source guard status for the specified interface

debug ip binding database

Command Objective This command specifies the debug levels for IP Binding Database module. The no form of this command disables IPDB module debugging.

Syntax **debug ip binding database {[entry][exit][debug][fail] | all}**

no debug ip binding database [{ [entry][exit][debug][fail] | all }]

Parameter Description

- `entry` - Generates debug statements for all function entry traces.
- `exit` - Generates debug statements for all function exit traces.
- `debug` - Generates debug statements for all debug traces.
- `fail` - Generates debug statements for all the failure traces.
- `all` - Generates debug statements for all the above mentioned traces.

Mode Privileged EXEC Mode

Example

```
Your Product# debug ip binding database entry
```

16 STP

STP (Spanning-Tree Protocol) is a link management protocol that provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations. To establish path redundancy, STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby or blocked state.

For an Ethernet network to function properly, only one active path should exist between two stations. Multiple active paths between stations in a bridged network can cause loops in which Ethernet frames can endlessly circulate. STP logically breaks such loops and prevents looping traffic from clogging the network. The dynamic control of the topology provides continued network operation in the presence of redundant or unintended looping paths.

The list of CLI commands for the configuration of STP is common to both SI and MI except for a difference in the prompt that appears for the switch with MI support. The prompt for the switch configuration Mode is,

Your Product(config-switch)# spanning-tree Mode rst

The STP functionality is realized in the network using one of the three following STPs:

- RSTP
- MSTP

STP Commands Common for RSTP and MSTP

This section describes all spanning tree protocol Related Commands that are common for all kinds of STPs.

RSTP

SMIS RSTP is an implementation of the IEEE 802.1D standard. It provides rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN. It reduces the time to reconfigure the active topology of the network when physical topology or topology configuration parameters changes. It provides increased availability of MAC service when there is a reconfiguration or failure of components in a bridged

LAN. It can interoperate with legacy STP bridges without any change in the configuration.

The list of common STP commands for the configuration of STP (RSTP / MSTP) is as follows:

- shutdown spanning-tree
- spanning-tree
- spanning-tree Mode
- spanning-tree compatibility
- spanning-tree timers
- spanning-tree transmit hold-count
- clear spanning-tree counters
- spanning-tree pathcost dynamic
- spanning-tree priority
- spanning-tree auto-edge
- spanning-tree - Properties of an interface
- spanning-tree portfast - disable | trunk
- spanning-tree portfast - bpdufilter default | bpduguarddefault | default
- spanning-tree restricted-role
- spanning-tree restricted-tcn
- spanning-tree layer2-gateway-port
- spanning-tree bpdu-receive
- spanning-tree bpdu-transmit
- spanning-tree loop-guard
- spanning-tree – Pseudoroot configuration
- debug spanning-tree
- clear spanning-tree detected protocols
- show spanning-tree - Summary, Blockedports, Pathcost, Redundancy
- show spanning-tree detail
- show spanning-tree active
- show spanning-tree interface
- show spanning-tree root
- show spanning-tree bridge
- show spanning-tree – layer 2 gateway port
- show customer spanning-tree
- spanning-tree forwarddelay optimization alternate-role

shutdown spanning-tree

Command Objective This command shuts down spanning tree functionality in the switch. The switch does not execute any kind of STP to form a loop free topology in the Ethernet network and operates with the existing topology structure.

Syntax **shutdown spanning-tree**

Mode Global Configuration Mode

Default Spanning tree MSTP is started and enabled in the switch.

Example `Your Product(config)# shutdown spanning-tree`

Related Command(s)

- `base bridge-Mode –` Configures the base Mode (either 802.1d transparent bridge Mode or 802.1q vlan aware bridge Mode) in which the VLAN feature should operate on the switch.
- `spanning-tree` - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree compatibility` - Sets the STP compatibility version in the switch for all ports.
- `spanning-tree timers` - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- `spanning-tree transmit hold-count` - Sets the transmit hold- count value for the switch.
- `clear spanning-tree counters` - Deletes all bridge and port level spanning tree statistics information.
- `spanning-tree pathcost dynamic` - Enables dynamic pathcost calculation feature in the switch.
- `spanning-tree priority` - Configures the priority value that is assigned to the switch.
- `spanning-tree auto-edge` - Enables automatic detection of Edge port parameter of an interface.
- `spanning-tree – Properties of an interface` - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- `spanning-tree restricted-role` - Enables the restricted role feature for a port.
- `spanning-tree restricted-tcn` - Enables the topology change guard / restricted TCN feature on a port.
- `spanning-tree layer2-gateway-port` - Configures a port to operate as a L2GP.
- `spanning-tree bpdu-receive` - Configures the processing status of the BPDUs received in a port.
- `spanning-tree bpdu-transmit` - Configures the BPDU transmission status of a port.
- `spanning-tree loop-guard` - Enables the loop guard feature in a port.
- `spanning-tree – Pseudoroot configuration` - Configures the pseudoroot related information for a port set as L2GP.
- `show spanning-tree` - Summary, Blockedports, Pathcost, redundancy - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.
- `show spanning-tree root` - Displays the spanning tree root information.
- `show spanning-tree bridge` - Displays the spanning tree bridge information.

- `show spanning-tree – layer 2 gateway port` - Displays spanning tree information for all L2GPs enabled in the switch.
- `spanning-tree mst max-hops` - Configures the maximum number of hops permitted in the MST.
- `spanning-tree mst configuration` - Enters into MST configuration Mode, where instance specific and MST region configuration can be done.
- `spanning-tree mst max-`instance - Configures the maximum number of active MSTIs that can be created.
- `spanning-tree mst- Properties of an interface for` MSTP - Configures the port related spanning tree information for a specified MSTI.
- `spanning-tree mst hello-time` - Configures the hello time for an interface that is enabled.
- `show spanning-tree mst - CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst configuration` - Displays multiple spanning tree instance related information.
- `show spanning-tree mst - Port Specific Configuration` - Displays multiple spanning tree port specific information for the specified port.
- `spanning-tree vlan` - Configures spanning tree related information on a per VLAN basis.
- `spanning-tree bpduguard` - Configures the status of BPDU guard feature in an interface.
- `spanning-tree guard` - Configures the various PVRST guard features such as root guard, in a port.
- `spanning-tree encap` - Configures the encapsulation type to be used in an interface.
- `spanning-tree vlan status` - Configures the status of PVRST on a port for the specified VLAN.
- `spanning-tree vlan port-priority` - Configures the priority of a port for the specified VLAN.
- `spanning-tree vlan cost` - Configures the cost of a port for the specified VLAN.
- `show spanning-tree vlan - Summary, Blockedports, Pathcost` - Displays PVRST related information for the specified VLAN.
- `show spanning-tree vlan - bridge` - Displays the PVRT related information of the bridge for the specified VLAN ID.
- `show spanning-tree vlan - root` - Displays the PVRT related information of the root, for the specified VLAN ID.
- `show spanning-tree vlan - interface` - Displays interface specific PVRST information for the specified VLAN.

spanning-tree

Command Objective This command enables the spanning tree operation in the switch for the selected spanning tree Mode.

The spanning tree operation provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations. It logically breaks such loops and prevents looping traffic from clogging the network.

The no form of this command disables the spanning tree operation in the switch. The spanning tree operation is automatically enabled in the switch, once the spanning tree Mode is changed.

Syntax **spanning-tree**

no spanning-tree

Mode Global Configuration Mode

Default Spanning tree MSTP is started and enabled in the switch.

The spanning tree operation can be enabled in the switch only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

```
Your Product(config)#spanning-tree
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree` - `Summary, Blockedports, Pathcost, redundancy` – Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.
- `show spanning-tree bridge` - Displays the spanning tree bridge information.
- `show spanning-tree mst - CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst - Port Specific Configuration` - Displays multiple spanning tree port specific information for the specified port.
- `show spanning-tree vlan - Summary, Blockedports, Pathcost` - Displays PVRST related information for the specified VLAN.
- `show spanning-tree vlan - interface` - Displays interface specific PVRST information for the specified VLAN.

spanning-tree Mode

This command sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch. The current selected type of spanning tree is enabled and the existing spanning tree type is disabled in the switch.

Syntax **spanning-tree Mode {mst|rst}**

no spanning-tree Mode

Parameter Description

- `mst` - Configures the switch to execute MSTP for preventing undesirable loops. MSTP configures spanning tree on per VLAN basis or multiple VLANs per spanning tree. The Mode cannot be set as mst, if the base bridge Mode is configured as transparent bridging.
- `rst` - Configures the switch to execute RSTP for preventing undesirable loops. RSTP provides rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN.

Mode Global Configuration Mode

Default mst

Example `Your Product(config)#spanning-tree Mode rst`

Related Command(s)

- `base bridge-Mode` - Configures the base Mode (either 802.1d transparent bridge Mode or 802.1q vlan aware bridge Mode) in which the VLAN feature should operate on the switch.
- `set gvrp disable` – Globally disables GVRP feature on all ports of a switch.
- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree` - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- `spanning-tree compatibility` - Sets the STP compatibility version in the switch for all ports.
- `spanning-tree timers` - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- `spanning-tree transmit hold-count` - Sets the transmit hold-count value for the switch.
- `clear spanning-tree counters` - Deletes all bridge and port level spanning tree statistics information.
- `spanning-tree pathcost dynamic` - Enables dynamic pathcost calculation feature in the switch.
- `spanning-tree priority` - Configures the priority value that is assigned to the switch.
- `spanning-tree auto-edge - Enables automatic detection of Edge port parameter of an interface.`
- `spanning-tree - Properties of an interface` - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- `spanning-tree restricted-role` - Enables the restricted role feature for a port.
- `spanning-tree restricted-tcn` - Enables the topology change guard / restricted TCN feature on a port.
- `spanning-tree layer2-gateway-port` - Configures a port to operate as a L2GP.
- `spanning-tree bpdu-receive` - Configures the processing status of the BPDUs received in a port.
- `spanning-tree bpdu-transmit` - Configures the BPDU transmission status of a port.
- `spanning-tree loop-guard` - Enables the loop guard feature in a port.
- `spanning-tree – Pseudoroot configuration` - Configures the pseudoroot related information for a port set as L2GP.
- `show spanning-tree - Summary, Blockedports, Pathcost, redundancy` - Displays spanning

tree related information available in the switch for the current STP enabled in the switch.

- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.
- `show spanning-tree root` - Displays the spanning tree root information.
- `show spanning-tree bridge` - Displays the spanning tree bridge information.
- `show spanning-tree – layer 2 gateway port` - Displays spanning tree information for all L2GPs enabled in the switch.
- `spanning-tree mst max-hops` - Configures the maximum number of hops permitted in the MST.
- `spanning-tree mst max-instance` - Configures the maximum number of active MSTIs that can be created.
- `spanning-tree mst configuration` - Enters into MST configuration Mode, where instance specific and MST region configuration can be done.
- `spanning-tree mst- Properties of an interface for MSTP` - Configures the port related spanning tree information for a specified MSTI.
- `spanning-tree mst hello-time` - Configures the hello time for an interface that is enabled.
- `show spanning-tree mst – CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst configuration` - Displays multiple spanning tree instance related information.
- `show spanning-tree mst – Port Specific Configuration` - Displays multiple spanning tree port specific information for the specified port.
- `spanning-tree vlan` - Configures spanning tree related information on a per VLAN basis.
- `spanning-tree bpduguard` - Configures the status of BPDU guard feature in an interface.
- `spanning-tree guard` - Configures the various PVRST guard features such as root guard, in a port.
- `spanning-tree encap` - Configures the encapsulation type to be used in an interface.
- `spanning-tree vlan status` - Configures the status of PVRST on a port for the specified VLAN.
- `spanning-tree vlan port-priority` - Configures the priority of a port for the specified VLAN.
- `spanning-tree vlan cost` - Configures the cost of a port for the specified VLAN.
- `show spanning-tree vlan - Summary, Blockedports, Pathcost` - Displays PVRST related information for the specified VLAN.
- `show spanning-tree vlan - bridge` - Displays the PVRT related information of the bridge for the specified VLAN ID.
- `show spanning-tree vlan - root` - Displays the PVRT related information of the root, for the specified VLAN ID.
- `show spanning-tree vlan - interface` - Displays interface specific PVRST information for the specified VLAN.
- `spanning-tree flush-interval` - Configures the flush interval timer value
- `spanning-tree flush-indication-threshold` - Configures the flush indication threshold value

for a specific instance.

- `spanning-tree forwarddelay optimization alternate-role` - enabels and disables the optimization for spanning-tree related protocol in alternate port role transition.

spanning-tree compatibility

Command Objective This command sets the STP compatibility version in the switch for all ports.

The no form of this command sets the STP compatibility version to its default value. The STP compatibility version is changed to its default value even if the spanning tree Mode is changed.

The compatibility version allows the switch to temporarily operate (that is, till this configuration is reset manually) in other STP version even though the spanning tree Mode is set as some other version. This configuration is useful during cases where spanning tree Mode itself is not required to be changed.

Syntax **spanning-tree compatibility {stp|rst|mst}**

no spanning-tree compatibility

Parameter Description

- `stp` - Configures the switch to execute spanning tree operation as specified in IEEE802.1D.
- `rst` - Configures the switch to execute spanning tree operation as specified in IEEE802.1w.
- `mst` - Configures the switch to execute spanning tree operation as specified in IEEE 802.1s. The STP compatibility version cannot be set as mst, if the spanning tree Mode is set as rst.

Mode Global Configuration Mode

Default

If STP Mode is set as mst, then spanning tree compatibility is set as mst.

If STP Mode is set as rst, then spanning tree compatibility is set as rst.

Notes:

The STP compatibility version can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

The STP compatibility version does not change the operation of the switch whose spanning tree Mode is set as PVRST.

Example

```
Your Product(config)#spanning-tree compatibility stp
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree

operation and starts spanning tree functionality in the switch.

- `show spanning-tree` - Summary, Blockedports, Pathcost, redundancy - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree vlan - Summary, Blockedports, Pathcost` - Displays PVRST related information for the specified VLAN.

spanning-tree timers

Command Objective This command sets the spanning tree timers such as hello time used for controlling the transmission of BPDUs during the computation of loop free topology.

The no form of this command resets the spanning tree timers to its default values. The spanning tree timers are reset to its default value, even if the spanning tree Mode is changed.

Syntax **spanning-tree {forward-time <seconds(4-30)> | hello-time <seconds(1-2)> | max-age <seconds(6-40)>}**

no spanning-tree { forward-time | hello-time | max-age }

Parameter Description

- `forward-time` - Configures the number of seconds, a port waits before changing from the blocking state to the forwarding state. This value ranges between 4 and 30 seconds. In MSTP, this time configuration is applied for IST root (that is, MSTI 0).
- `hello-time` - Configures the time interval (in seconds) between two successive configuration BPDUs generated by the root switch. This value should be either 1 or 2 seconds. This value is configured on per-port basis for MSTP and is configured globally for RSTP.
- `max-age` - Configures the maximum expected arrival time (in seconds) of hello BPDUs. STP information learned from network on any port is discarded, once the configured arrival time expires. The spanning tree topology is re-computed after this time interval. This value ranges between 6 and 40 seconds. In MSTP, this time configuration is applied for IST root(that is, MSTI0).

Note: Spanning-tree timers can be configured in centi seconds through SNMP

Mode Global Configuration Mode

Default

- `forward-time` - 15 seconds
- `hello-time` - 2 seconds
- `max-age` - 20 seconds

Notes:

The values configured for the spanning tree timers should satisfy the following conditions:

```
2 * (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1)
```

The STP timers can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

This spanning tree timer's configuration is not supported in PVRST Mode.

Example `Your Product(config)#spanning-tree max-age 6`

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree - Summary, Blockedports, Pathcost, redundancy` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree interface detail` - Displays detailed spanning tree related information for the specified port.
- `show spanning-tree root` - Displays the spanning tree root information.
- `show spanning-tree bridge` - Displays the spanning tree bridge information.
- `show spanning-tree mst - CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst - Port Specific Configuration` - Displays multiple spanning tree port specific information for the specified port.

spanning-tree transmit hold-count

Command Objective This command sets the BPDU transmit hold-count value for the switch. The transmit hold count value is a counter that is used to limit the maximum BPDU transmission rate of the switch and to avoid flooding. This value specifies the maximum number of BPDU packets that can be sent in a given hello time interval. This value ranges between 1 and 10.

The no form of this command sets the transmit hold-count to its default value. The transmit hold-count is changed to its default value even if the spanning tree Mode is changed.

Syntax **spanning-tree transmit hold-count <value (1-10)>**

no spanning-tree transmit hold-count

Mode Global Configuration Mode

Default 6, if the Spanning Tree Mode is set as mst.

3, if the Spanning Tree Mode is set as rst or pvrst.

The transmit hold-count value can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

This transmit hold count value configuration is not supported in PVRST Mode.

Example

```
Your Product(config)#spanning-tree transmit hold-count 5
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables `spanning tree` operation and starts spanning tree functionality in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree vlan - Summary, Blockedports, Pathcost` - Displays PVRST related information for the specified VLAN.

clear spanning-tree counters

Command Objective This command deletes all bridge and port level spanning tree statistics information.

For RSTP, the information contains the number of:

- Transitions to forwarding state
- RSTP BPDU count received / transmitted
- Config BPDU count received / transmitted
- TCN BPDU count received / transmitted
- Invalid BPDU count transmitted
- Port protocol migration count

For MSTP, the information contains number of:

- Port forward transitions
- Port received BPDUs
- Port transmitted BPDUs
- Port invalid BPDUs received
- Port protocol migration count
- BPDUs sent / received for each MSTI

Syntax **clear spanning-tree [mst <instance-id>] counters[interface <interface-type> <interface-id>]**

Parameter Description

- `mst <instance-id>]` - Clears the statistical counters specific to the MSTP instance already created in the switch. This value ranges between 1 and 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs. This option is applicable, only if the spanning tree Mode is set as mst.
- `interface` - Clears all port-level spanning-tree statistics information for the given port.
  - `<interface-type>` - Clears all port-level spanning-tree statistics information for the specified type of interface. The interface can be:
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
    - `qx-ethernet` – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
  - `<interface-id>` - Clears all port-level spanning-tree statistics information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 representsthat the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface types port-channel. For example: 1 represents port-channel ID.

Mode Global Configuration Mode

The statistics information can be deleted, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

```
Your Product(config)# clear spanning-tree mst 1 counters
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `instance` - Creates an MST instance and maps it to VLANs.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.

- `show spanning-tree active detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.
- `show spanning-tree mst - CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst - Port Specific Configuration` - Displays multiple spanning tree port specific information for the specified port.
- `show spanning-tree vlan - Summary, Blockedports, Pathcost` - Displays PVRST related information for the specified VLAN.
- `show spanning-tree vlan - interface` - Displays interface specific PVRST information for the specified VLAN.

spanning-tree pathcost dynamic

Command Objective This command enables dynamic pathcost calculation feature in the switch.

The no form of this command disables dynamic pathcost calculation feature in the switch. The dynamic pathcost calculation feature is disabled, even if the spanning tree Mode is changed.

The path cost of the port / MSTI is dynamically calculated. This feature is applied only for the ports that are not shutdown during the execution of STP. The calculated path cost is not changed based on the operational status of the port / for a MSTI, once calculated. The manually assigned / already calculated path cost is used even if the dynamic pathcost calculation feature is enabled in the switch.

Syntax **spanning-tree pathcost dynamic [lag-speed]**

no spanning-tree pathcost dynamic [lag-speed]

Parameter Description `lag-speed` - Calculates the path cost for change in speed of the port. This feature is used for LA ports whose speed changes due to addition or deletion of ports from the port channel. The manually assigned path cost is used even if the lag speed feature is enabled in the switch, if the path cost is assigned manually. The lag speed feature can be enabled, only after enabling the dynamic pathcost calculation feature.

Mode Global Configuration Mode

Default Dynamic pathcost calculation feature is disabled in the switch.

Note: The dynamic pathcost calculation feature can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

```
Your Product(config)# spanning-tree pathcost dynamic
```

Related Command(s)

- shutdown spanning-tree - Shuts down spanning tree functionality in the switch.
- spanning-tree Mode - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- spanning-tree - Properties of an interface - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- show spanning-tree - Summary, Blockedports, Pathcost, redundancy – Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- show spanning-tree detail - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- show spanning-tree active - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- spanning-tree mst- Properties of an interface for MSTP - Configures the port related spanning tree information for a specified MSTI.
- spanning-tree vlan cost - Configures the cost of a port for the specified VLAN.

spanning-tree priority

Command Objective This command configures the priority value that is assigned to the switch.

The no form of this command resets the priority to its default value. The priority value is changed to its default value even if the spanning tree Mode is changed.

In RSTP, this value is used during the election of root. In MSTP, this value is used during the election of CIST root, CIST regional root and IST root.

Syntax **spanning-tree [mst <instance-id>] priority <value(0-61440)>**

no spanning-tree [mst <instance-id(1-64)>] priority

Parameter Description

- mst <instance-id> - Configures the ID of MSTP instance already created in the switch. This value ranges between 1 and 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs. This option is applicable, only if the spanning tree Mode is set as mst.
- priority <value(0-61440)> - Configures the priority value for the switch and for the MSTI, in RSTP and MSTP respectively. This value ranges between 0 and 61440. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.

Mode Global Configuration Mode

Default priority - 32768

Note: The priority value can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

This priority value configuration is not supported in PVRST Mode.

Example `Your Product(config)#spanning-tree priority 4096`

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree root` - Displays the spanning tree root information.
- `show spanning-tree bridge` - Displays the spanning tree bridge information.
- `show spanning-tree` - Summary, Blockedports, Pathcost, redundancy – Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `instance` - Creates an MST instance and maps it to VLANs.
- `show spanning-tree mst - CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst - Port Specific Configuration` - Displays multiple spanning tree port specific information for the specified port.

spanning-tree auto-edge

Command Objective This command enables automatic detection of Edge port parameter of an interface.

The no form of this command disables automatic detection of Edge port parameter of an interface. The automatic detection of Edge port parameter is disabled, even if the spanning tree Mode is changed.

Once automatic detection is enabled, the Edge port parameter is automatically detected and set. The port is set as edge port, if no BPDU is received on the port. The port is set as non-edge port, if any BPDU is received.

Syntax **spanning-tree auto-edge**

no spanning-tree auto-edge

Mode Interface Configuration Mode (Physical Interface Mode)

Default Automatic detection of Edge port parameter of an interface is enabled.

The automatic detection of Edge port parameter can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example `Your Product(config-if)# spanning-tree auto-edge`

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.

spanning-tree - Properties of an interface

Command Objective This command configures the port related spanning tree information for all kinds of STPs. This can be applied for any port, in RSTP/MSTP Mode. This command creates port in STP when Automatic Port Create feature is disabled.

The no form of this command resets the port related spanning tree information to its default value. The port related spanning tree information is changed to its default value even if the spanning tree Mode is changed. This command also deletes port in STP when Automatic Port Create feature is disabled.

Note: In STP module, whenever a port is mapped to any context, the corresponding port is created irrespective of whether STP is intended to be enabled on that interface. This leads To STP scaling issues and this problem is solved by having control at STP module on the port entry creation at STP module itself.

Syntax **spanning-tree [{cost <value(0-200000000)>|disable|link- type{point-to-point|shared}|portfast|port-priority <value(0-240)>}]**

no spanning-tree [{cost |disable|link-type|portfast|port- priority}]

Parameter Description

- `cost <value(0-200000000)>` - Configures the port's path cost value that contributes to the path cost of paths containing this particular port. The paths' path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. This value ranges between 1 and 200000000. The configured path cost is used, even if the dynamic pathcost calculation feature or LAGG speed feature is enabled. This configuration is not supported for the spanning tree Mode pvrst.
- `disable` - Disables the spanning tree operation on the port. The port does not take part in the execution of spanning tree operation for preventing undesirable loops in the network.
- `link-type` - Configures the link status of the LAN segment attached to the port. The options available are:
  - `point-to-point` – The port is treatedas if it is connected to a point-to-point link.
  - `shared` - The port is treated as if it is using a shared media connection.
- `portfast` - Configures the portfast feature in the port. This feature specifies that the port is connected to only one hosts and hence can rapidly transit to forwarding. This feature can cause temporary bridging loops, if hubs, concentrators, switches, bridges and so on are connected to this

port. This feature takes effect only when the interface is shutdown.

- `port-priority <value(0-240)>` - Configures the priority value assigned to the port. This value is used during port role selection process. This value ranges between 0 and 240. This value should be set in steps of 16, that is, you can set the value as 0, 16, 32, 48, and so on. This configuration is not supported for the spanning tree Mode pvrst.

Mode Interface Configuration Mode (Physical Interface Mode)

Default

- `cost` - 200000 for all physical ports, 199999 for port channels
- `disable` - Spanning tree operation is enabled in the port.
- `link-type` - The port is considered to have a point-to-point link if:
    - It is an aggregator and all of its members can be aggregated.
    - The MAC entity is configured for full duplex operation, either manually or through auto negotiation process (that is, negotiation Mode is set as Auto)
    - Otherwise port is considered to have a shared media connection
- `portfast` - Portfast is disabled.
- `port-priority` - 128

Notes:

1. The port-related spanning tree information can be configured, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.
2. This command executes without the optional parameters only if automatic port- create feature is disabled.

Example

```
Your Product(config-if)# spanning-tree cost 2200
Your Product(config-if)# spanning-tree link-type point-to- point
Your Product(config-if)# spanning-tree portfast
Your Product(config-if)# spanning-tree port-priority 32
Your Product(config-if)# spanning-tree
```

Related Command(s)

- `automatic-port-create` - Enables or disables the Automatic Port Create feature.
- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree pathcost dynamic` - Enables dynamic pathcost calculation feature in the switch.
- `show spanning-tree - Summary, Blockedports, Pathcost, redundancy` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch

for the current STP enabled in the switch.

- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.
- `show spanning-tree root` - Displays the spanning tree root information.
- `show spanning-tree mst - CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst - Port Specific Configuration` - Displays multiple spanning tree port specific information for the specified port.
- `show spanning-tree vlan - Summary, Blockedports, Pathcost` - Displays PVRST related information for the specified VLAN.

spanning-tree portfast - disable | trunk

Command Objective This command configures the portfast Mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire.

Notes:

1. This command is a standardized implementation of the existing command; spanning-tree - Properties of an interface. It operates similar to the existing command.
2. The spanning-tree portfast feature is currently not supported in the Global Configuration Mode.

Syntax **spanning-tree portfast { disable | trunk}**

Parameter Description

- `disable` - Disables PortFast Mode
- `trunk` - Enables PortFast Mode

Mode Global Configuration Mode

Example

```
Your Product(config)# spanning-tree portfast trunk
```

Related Command(s)

- `spanning-tree Mode -pvrst` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree interface` - Displays the spanning tree port specific configuration.

spanning-tree portfast - bpdufilter default | bpduguarddefault | default

Command Objective This command configures the portfast of the non-trunk ports as bpdufilter default or bpduguard default or default. This is used only for Trunk ports.

Notes:

1. This command is a standardized implementation of the existing command; spanning-tree - Properties of an interface. It operates similar to the existing command.
2. The spanning-tree portfast feature is currently not supported in the Global Configuration Mode.

Syntax **spanning-tree portfast {bpdufilter default | bpduguard default | default}**

no spanning-tree portfast {bpdufilter default | bpduguard default | default}

Parameter Description

- `bpdufilter default` - Enables BPDU filtering on all PortFast ports.
- `bpduguard default` - Enables BPDU guard feature on all PortFast ports.
- `default` - Enables PortFast by default on all access ports.

Mode Global Configuration Mode

Example

```
Your Product(config)# spanning-tree portfast default
```

Related Command(s)

- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree interface` - Displays the spanning tree port specific configuration.

spanning-tree restricted-role

Command Objective This command enables the restricted role feature for a port.

The restricted role feature blocks the port from being selected as a root port even if it has the best spanning tree priority vector. This port is selected as an alternate port after the root port is selected. This feature allows you to block switches external to a core region of the network from influencing the spanning tree active topology.

The blocking of port from being selected as a root port can cause lack of spanning tree connectivity.

The no form of this command disables the restricted role feature in the port. The restricted role feature is disabled, even if the spanning tree Mode is changed or port is set as L2GP.

Syntax **spanning-tree restricted-role**

no spanning-tree restricted-role

Mode Interface Configuration Mode (Physical Interface Mode)

Default Restricted role feature is disabled in all ports.

The restricted role feature can be configured, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

This configuration is not supported in PVRST Mode.

Example `Your Product(config-if)# spanning-tree restricted-role`

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree layer2-gateway-port` - Configures a port to operate as a L2GP.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.

spanning-tree restricted-tcn

Command Objective This command enables the topology change guard / restricted TCN feature on a port.

The restricted TCN feature blocks the port from propagating the received topology change notifications and topology changes to other ports. This feature allows you to block switches external to a core region of the network from causing address flushing in the region.

The blocking of port can cause temporary loss of connectivity after changes in a spanning tree active topology as a result of persistent incorrectly learnt station location information.

The no form of this command disables the topology change guard / restricted TCN feature on the port. The topology change guard / restricted TCN feature is disabled, even if the spanning tree Mode is changed or port is set as L2GP.

Syntax **spanning-tree restricted-tcn**

no spanning-tree restricted-tcn

Mode Interface Configuration Mode (Physical Interface Mode)

Default Topology change guard / restricted TCN feature is disabled in all ports..

Notes:

1. The topology change guard / restricted TCN feature can be configured, only if the

spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

2. This configuration is not supported in PVRST Mode.

Example `Your Product(config-if)# spanning-tree restricted-tcn`

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree layer2-gateway-port` - Configures a port to operate as a L2GP.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.

spanning-tree layer2-gateway-port

Command Objective This command configures a port to operate as a L2GP.

L2GP operates similar to that of the normal port operation but pretends to continuously receive BPDUs when admin state of the port is Up.

The no form of this command configures the port to operate as a normal port. The port operates as normal port, even if the spanning tree Mode is changed.

Syntax **spanning-tree layer2-gateway-port**

no spanning-tree layer2-gateway-port

Mode Interface Configuration Mode (Physical Interface Mode)

Default The port operates as a normal port.

Notes:

1. The port can be configured as L2GP, only if the BPDU transmit status, restricted role feature and restricted TCN feature of the port are disabled.
2. The PIP or CBP ports cannot be set as L2GP.
3. Ports with SISP enabled interfaces cannot be set as L2GP.
4. The port state of the L2GP is always set as discarding.
5. The topology change guard / restricted TCN feature can be configured, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree

Mode should be set, if the functionality is already shutdown.

Example `Your Product(config-if)# spanning-tree layer2-gateway-port`

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree restricted-role - Enables the restricted role feature for a port.`
- `spanning-tree restricted-tcn` - Enables the topology change guard / restricted TCN feature on a port.
- `spanning-tree bpdu-transmit` - Configures the BPDU transmission status of a port.
- `show spanning-tree` - Summary, Blockedports, Pathcost, redundancy - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` – Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.
- `show spanning-tree – layer 2 gateway port` - Displays spanning tree information for all L2GPs enabled in the switch.
- `show spanning-tree mst – CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst – Port Specific Configuration` - Displays multiple spanning tree port specific information for the specified port.
- `show spanning-tree vlan - Summary, Blockedports, Pathcost` - Displays PVRST related information for the specified VLAN.
- `show spanning-tree vlan - interface` - Displays interface specific PVRST information for the specified VLAN.

spanning-tree bpdu-receive

Command Objective This command configures the processing status of the BPDUs received in a port. BPDUs are used to carry bridge related information that is used during spanning tree operation.

The processing status is reset to its default value, once the spanning tree Mode is changed.

Syntax **spanning-tree bpdu-receive {enabled | disabled}**

Parameter Description

- `enabled` - Allows normal processing of BPDUs received on the port.
- `disabled` - Discards the BPDUs received on the port.

Mode Interface configuration Mode (Physical Interface Mode)

Default enabled

Note: The processing status of the received BPDUs can be configured, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

```
Your Product(config-if)# spanning-tree bpdu-receive disabled
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.

- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.

- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.

- `show spanning-tree active detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.

- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.

spanning-tree bpdu-transmit

Command Objective This command configures the BPDU transmission status of a port. BPDUs are used to carry bridge related information that is used during spanning tree operation.

The transmission status is reset to its default value, once the spanning tree Mode is changed.

Syntax **spanning-tree bpdu-transmit {enabled | disabled}**

Parameter Description

- **`enabled`** - Allows the transmission of BPDUs from the port.
- `disabled` - Blocks the transmission of BPDUs from the port.

Mode Interface configuration Mode (Physical Interface Mode)

Default enabled

Notes:

1. BPDU transmission status cannot be enabled on the port that is configured as L2GP.
2. The BPDU transmission status can be configured, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

```
Your Product(config-if)# spanning-tree bpdu-transmit enabled
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree layer2-gateway-port` - Configures a port to operate as a L2GP.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.

spanning-tree loop-guard

Command Objective This command enables the loop guard feature in a port.

This feature prevents the alternative or root ports from becoming designated ports due to failure in a unidirectional link. This feature is useful when the neighbor bridge is faulty, that is, the bridge cannot send BPDUs but continues to send data traffic.

The no form of this command disables the loop guard feature in the port. The loop guard feature is disabled, even if the spanning tree Mode is changed.

Syntax **spanning-tree loop-guard**

no spanning-tree loop-guard

Mode Interface Configuration Mode (Physical Interface Mode)

Package Workgroup, Enterprise Metro_E and Metro

Note: The loop guard feature can be configured, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

```
Your Product(config-if)# spanning-tree loop-guard
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.

spanning-tree – Pseudoroot configuration

Command Objective This command configures the pseudoroot related information for a port set as L2GP.

The information contains pseudoroot priority and pseudoroot MAC address for the port. This configuration is not utilized in PVRST Mode.

The no form of this command resets the pseudoroot related information to the currently available bridge related information.

Syntax **spanning-tree [mst <instance-id>] pseudoRootId priority <value(0-61440)> mac-address <ucast_mac>**

no spanning-tree [mst <instance-id(1-64)>] pseudoRootId

Parameter Description

- `mst <instance-id>/ mst <instance-id(1-64)>` - Configures the ID of MSTP instance already created in the switch. This value ranges between 1 and 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs. This option is applicable, only if the spanning tree Mode is set as mst.
- `priority <value(0-61440)>` - Configures the priority of the pseudoroot. Port configured as L2GP uses this value in generated BPDUs as the root identifier. This value ranges between 0 and 61440. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.
- `mac-address` - Configures the unicast MAC address of the pseudoroot. Port configured as L2GP uses this value as its address.

Mode Interface configuration Mode (Physical Interface Mode)

Default

- `priority` - Priority value assigned to the switch.
- `mac-address` - MAC address assigned to the switch.

Note: The pseudoroot related information can be configured, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example `Your Product(config-if)# spanning-tree mst 1 pseudoRootId priority 8192 mac-address 00:00:12:34:45:55`

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree interface` – Displays the port related spanning tree information for the specified interface.
- `show spanning-tree – layer 2 gateway port` - Displays spanning tree information for all L2GPs enabled in the switch.
- `instance` - Creates an MST instance and maps it to VLANs.
- `show spanning-tree mst – CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst – Port Specific Configuration` – Displays multiple spanning tree port specific information for the specified port.
- `show spanning-tree vlan - Summary, Blockedports, Pathcost - Displays PVRST related information for the specified VLAN.`
- `show spanning-tree vlan – interface` - Displays interface specific PVRST information for the specified VLAN.

debug spanning-tree

Command Objective This command enables the tracing of the STP module as per the configured debug levels. The trace statements are generated for the configured trace levels.

This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

The no form of this command disables the tracing of the STP module as per the configured debug levels. The trace statements are not generated for the configured trace levels.

Syntax **debug spanning-tree { global | all | [errors] [init-shut] [management] [memory] [bpdu] [events] [timer] [port-info- state-machine] [port-recieve-state-machine] [port-role-selection-state-machine] [role-transition-state-machine] [state-transition-state-machine]**

[protocol-migration- state-machine] [topology-change-state-machine] [port- transmit-state-machine] [bridge-detection-state-machine] [pseudoInfo-state-machine] [redundancy] [sem-variables] [switch <context_name>]}

no debug spanning-tree {global | {all | errors | init-shut | management | memory | bpdu |events | timer | state- machine {port-info | port-receive | port-role-selection | role-transition | state-transition | protocol-migration | topology-change | port-transmit | bridge-detection | pseudoInfo } redundancy | sem-variables} [switch <context_name>]}

Parameter Description

- `global` - Generates debug statements for global traces. This trace is used for providing status of STP task initialization, memory-pool creation and event-reception in STP task.

  `Note`: This parameter is specific to Multiple Instance.

- `all` - Generates debug statements for all kinds of traces.
- `errors` - Generates debug statements for all failure traces.
- `init-shut` - Generates debug statements for init and shutdown traces. This trace is generated on failed and successful initialization and shutting down of STP related module and memory.
- `management` - Generates debug statements for management traces. This trace is generated whenever you configure any of the STP features.
- `memory` - Generates debug statements for memory related traces. This trace is generated on failed and successful allocation of memory for STP process.
- `bpdu` - Generates debug statements for BPDU related traces. This trace is generated on failed and successful reception, transmission and processing of BPDUs.
- `events` - Generates debug statements for event handling traces. This trace is generated to denote events that are posted to STP configuration queue whenever you configure any of the STP features.
- `timer` - Generates debug statements for timer module traces. This trace is generated on failed and successful start, stop and restart of STP timers.
- `port-info-state-machine` - Generates debug statements for port information SEM.
- `port-recieve-state-machine` - Generates debug statements for port receive SEM.
- `port-role-selection-state-machine` - Generates debug statements for role selection SEM.
- `role-transition-state-machine` - Generates debug statements for role transition SEM.
- `state-transition-state-machine` - Generates debug statements for state transition SEM.
- `protocol-migration-state-machine` - Generates debug statements for protocol migration SEM.
- `topology-change-state-machine` - Generates debug statements for topology change SEM.
- `port-transmit-state-machine` - Generates debug statements for port transmit SEM.
- `bridge-detection-state-machine` - Generates debug statements for bridge detection SEM.
- `pseudoInfo-state-`machine - Generates debug statements for port receive pseudo information SEM.
- `state machine` - Generates debug statements to denote the event and state of the selected SEM. The options are:

- `port-info` - Generates debug statements for port information SEM.
    - `port-receive` - Generates debug statements for port receive SEM.
    - `port-role-selection` - Generates debug statements for role selection SEM.
    - `role-transition` - Generates debug statements for role transition SEM.
    - `state-transition` – Generates debug statements for state transition SEM.
    - `protocol-migration` - Generates debug statements for protocol migration SEM.
    - `topology-change` - Generates debug statements for topology change SEM.
    - `port-transmit` - Generates debug statements for port transmit SEM.
    - `bridge-detection` - Generates debug statements for bridge detection SEM.
    - `pseudoInfo` - Generates debug statements for port receive pseudo information SEM.
- `redundancy` - Generates debug statements for redundancy code flow traces. This trace is generated in standby node STP while taking backup of configuration information from active node.
- `sem-variables` - Generates debug statements for state machine variable changes traces. This trace is generated on failed and successful creation and deletion of semaphore.
- `switch<context_name>` - Configures the tracing of the STP module for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Default Tracing of the STP module is disabled

Example `Your Product# debug spanning-tree all`

clear spanning-tree detected protocols

Command Objective This command restarts the protocol migration process on all interfaces in the switch and forces renegotiation with the neighboring switches.

Syntax **clear spanning-tree detected protocols [{interface <interface-type> <interface-id> | switch <context_name>}]**

Parameter Description

- `interface <interface-type> <interface-id>` - Restarts the protocol migration process on the specified interface. The details to be provided are:
    - `interface-type>` - Sets the type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.

- `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface types port-channel.

- `switch <context_name>` - Restarts the protocol migration process for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# clear spanning-tree detected protocols interface
gigabitethernet 0/1
```

Related Command(s) `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.

show spanning-tree - Summary, Blockedports, Pathcost, Redundancy

Command Objective This command displays spanning tree related information available in the switch for the current STP enabled in the switch.

The information contain priority, address and timer details for root and bridge, status of dynamic pathcost calculation feature, status of spanning tree function, STP compatibility version used, configured spanning tree Mode, bridge and port level spanning tree statistics information, and details of ports enabled in the switch. The port details contain port ID, port role, port state, port cost, port priority and link type.

Syntax **show spanning-tree [{ summary | blockedports | pathcost method | redundancy }] [switch <context_name>]**

Parameter Description

- `summary` - Displays the currently used STP, applied path cost method and port details such as port ID, port role, port state and port status. This option cannot be executed in the PVRST Mode.
- `blockedports` - Displays the list of ports in blocked state and the total number of blocked ports. This option cannot be executed in the PVRST Mode.
- `pathcost method` - Displays the port pathcost method configured for the switch.
- `redundancy` - Displays the port role and port state, and dumps the STP port related information.
- `switch <context_name>` - Displays the STP related information in the switch, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Note: This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

```
Single Instance:
Your Product# show spanning-tree
Root Id        Priority 32768
Address 00:01:02:03:04:01
Cost 0
Port 0 [0]
This bridge is the root
Max age 20 Sec 0 cs, forward delay 15 Sec 0 cs
Hello Time 2 sec 0 cs
MST00
Spanning tree Protocol has been enabled
MST00 is executing the mstp compatible Multiple Spanning
Tree Protocol
Bridge     Id Priority 32768
             Address 00:01:02:03:04:01
             Max age is 20 sec, forward delay is  15 sec
Dynamic Path Cost is Disabled
Name       Role            State        Cost         Prio   Type
-------------------------------------------------------------   ---------   ----------------
Gi0/1      Designated      Forwarding   200000       128    SharedLan
Gi0/2      Designated      Forwarding   200000       128    SharedLan
Gi0/3      Designated      Forwarding   200000       128    SharedLan
Gi0/4      Designated      Forwarding   200000       128    SharedLan
Gi0/5      Designated      Forwarding   200000       128    SharedLan
Gi0/6      Designated      Forwarding   200000       128    SharedLan
Gi0/7      Designated      Forwarding   200000       128    SharedLan
Your Product# show spanning-tree blockedports
Blocked Interfaces List:
The Number of Blocked Ports in the system is :1
Your Product# show spanning-tree pathcost method
Spanning Tree port pathcost method is Long
Your Product# show spanning-tree summary
Spanning tree enabled protocol is RSTP
Spanning Tree port pathcost method is Long
RSTP Port Roles and States
             Port-Index   Port-Role     Port-State     Port-Status

             ----------   ----------    ------------   ------------
             1            Designated    Forwarding     Enabled

             2            Designated    Forwarding     Enabled

             3            Designated    Forwarding     Enabled

             4            Designated    Forwarding     Enabled

             5            Designated    Forwarding     Enabled

Your Product# show spanning-tree redundancy
Port Role/State for Instance 0 Port 1
```

```
======================
Port Role 3 Port State 5
Port Role/State for Instance 0 Port 2
Port Role 1 Port State 2
Dumping Data On Port 1
--------------------------------------
RootId 0:00:11:22:33:44:55
Designated BrId 0:00:11:22:33:44:55
Root path Cost 0
Length 0
Protocol Id 0
Port Id 8001
Message Age 0
Max Age 14
Hello Time 2
Fwd Delay Time 15
Dest Addr 00:00:00:00:00:00
Src Addr 00:00:00:00:00:00
Version Length 0
Version 2
BPDU Type 2
Flags e
Dumping Data On Port 2
--------------------------------------
RootId 0:00:11:22:33:44:55
Designated BrId 0:00:11:22:33:44:55
Root path Cost 0
Length 0
Protocol Id 0
Port Id 8002
Message Age 0
Max Age 14
Hello Time 2
Fwd Delay Time 15
Dest Addr 00:00:00:00:00:00
Src Addr 00:00:00:00:00:00
Version Length 0
Version 2
BPDU Type 2
Flags e
Instance 0 Port 1
======================
Expected FdWile expiry time 0
Expected rcvdInfo exp Time 4654
Expected rrWhile exp Time 0
Expected rbWhile exp Time 0
Expected tcWhile exp Time 0
Instance 0 Port 1
TCN Var 1
STP Version 1
Proposing Flag 0
Info Is 4
Instance 0 Port 2
======================
Expected FdWile expiry time 0
Expected rcvdInfo exp Time 4656
Expected rrWhile exp Time 0
Expected rbWhile exp Time 0
Expected tcWhile exp Time 0
Instance 0 Port 2
TCN Var 1
STP Version 1
Proposing Flag 0
Info Is 4
Multiple Instance: For RSTP
Your Product# show spanning-tree
Switch default
We are the root of the Spanning Tree
Root Id    Priority 32768
Address    00:05:02:03:04:01
Cost         0
Port         0
Max Age 20 sec 0 cs, Forward Delay 15 sec 0 cs
Bridge is executing the rstp compatible Rapid Spanning Tree
Protocol
Bridge Id Priority 32768
Address 00:05:02:03:04:01
Hello Time 1 sec 58 cs, Max Age 20 sec 0 cs
Forward Delay 15 sec 0 cs
Dynamic Path Cost is Disabled
Dynamic Path Cost Lag-Speed Change is
Disabled
Name       Role     State  Cost   Prio   Type
-------    -------  -------- -------  -------  ----------
For MSTP
Your Product# show spanning-tree
Switch default
Root Id        Priority  32768
Address   00:01:02:03:04:01
Cost      0
Port      0 [0]
This bridge is the root
Max age 20 Sec 0 cs, forward delay 15 Sec 0 cs
Hello Time is 2 sec 0 cs
MST00
Spanning tree Protocol Enabled.
S-VLAN Component: MST00 is executing the mstp compatible
Multiple Spanning Tree
Protocol
Bridge Id Priority 32768
Address 00:01:02:03:04:01
Max age 20 Sec 0 cs, forward delay 15 Sec 0 cs
Hello Time is 2 sec 0 cs
Name       Role            State        Cost         Prio   Type
                           --------     -------

Gi0/1      Disabled Discarding   200000       128    SharedLan
Gi0/2      Designated      Forwarding   200000       128    SharedLan
Gi0/3      Designated      Forwarding   200000       128    SharedLan
Gi0/4      Designated      Forwarding   200000       128    SharedLan
Gi0/5      Designated      Forwarding   200000       128    SharedLan
```

```
Gi0/6      Designated      Forwarding   200000        128    SharedLan
Gi0/7      Designated      Forwarding   200000        128    SharedLan
Your Product# show spanning-tree summary
Switch - default
Spanning Tree port pathcost method is Long
Spanning tree enabled protocol is MSTP
MST00 Port Roles and States
Port-Index Port-Role Port-State    Port-Status
---------------- ------------------------------    -----------------
49           Disabled     Forwarding   Disabled
Switch - cust1
Spanning Tree port pathcost method is Long
Spanning tree enabled protocol is MSTP
MST00 Port Roles and States
Port-Index Port-Role Port-State    Port-Status
---------------- ------------------------------    -----------------
1            Designated   Forwarding   Enabled
2            Root         Forwarding   Enabled
3            Designated   Forwarding   Enabled
4            Disabled     Discarding   Enabled
5            Disabled     Discarding   Enabled
6            Disabled     Discarding   Enabled
Switch - cust2
Spanning Tree port pathcost method is Long
Spanning tree enabled protocol is MSTP
MST00 Port Roles and States
Port-Index Port-Role Port-State    Port-Status
------------------ -------------------------------------------------------------------
7            Designated   Forwarding   Enabled
8            Root         Forwarding   Enabled
9            Alternate    Discarding   Enabled
10           Disabled     Discarding   Enabled
11           Disabled     Discarding   Enabled
12           Disabled     Discarding   Enabled
```

Related Command(s)

- `shutdown` - physical/VLAN/port-channel/tunnel Interface - Disables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.
- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree` - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree compatibility` - Sets the STP compatibility version in the switch for all ports.
- `spanning-tree timers` - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- `spanning-tree pathcost dynamic` - Enables dynamic pathcost calculation feature in the switch.
- `spanning-tree priority` - Configures the priority value that is assigned to the switch.
- `spanning-tree - Properties of an interface` - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.

- `spanning-tree layer2-gateway-port` - Configures a port to operate as a L2GP.
- `spanning-tree mst` - Properties of an interface for MSTP - Configures the port related spanning tree information for a specified MSTI.
- `spanning-tree mst hello-time` - Configures the hello time for an interface that is enabled.
- `spanning-tree vlan` - Configures spanning tree related information on a per VLAN basis.
- `spanning-tree vlan status` - Configures the status of PVRST on a port for the specified VLAN.
- `spanning-tree vlan port-priority` - Configures the priority of a port for the specified VLAN.
- `spanning-tree vlan cost` - Configures the cost of a port for the specified VLAN.

show spanning-tree detail

Command Objective This command displays detailed spanning tree related information of the switch and all ports enabled in the switch.

The information contains status of spanning tree operation, current selected spanning Mode, current spanning tree compatibility version, bridge and root priority, bridge and root addresses, port path cost, port priority, port timers, bridge and port level spanning tree statistics information, transmit hold-count value, link-type, and status of L2GP, loop guard, BPDU receive, BPDU transmit, restricted TCN, restricted role and portfast features.

Syntax **show spanning-tree detail [switch <context_name>]**

Parameter Description `switch <context_name>` - Displays detailed spanning tree related information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Note: This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

```
Single Instance
Your Product# show spanning-tree detail
Spanning tree Protocol Enabled.
Bridge is executing the rstp compatible Spanning Tree
Protocol

Bridge Identifier has priority 32768, Address
00:01:02:03:04:01
Configured Hello time 2 sec 0 cs, Max Age 20 sec 0 cs, Forward Delay 15 sec
0 cs
Dynamic Path Cost Disable
We are the root of the spanning tree
Number of Topology Changes 0
Time since topology Change 0 seconds ago
Transmit Hold-Count 6
```

```
Root Times:Max Age 20 sec 0 cs  Forward Delay 15 sec 0 cs
Hello Time 2 sec 0 cs
Port 1 [Gi0/1] is Designated, Discarding
Port PathCost 200000, Port Priority 128, Port Identifier
128.1
Designated Root has priority 32768, address
00:01:02:03:04:01
Designated Bridge has priority 32768, address
00:01:02:03:04:01
Designated Port Id is 128.1, Designated PathCost 0
No of Transitions to forwarding State :0
PortFast is disabled
Link Type is Shared
BPDUs : sent 3 , recieved 0
Timers: Hello - 1, Forward Delay - 14, Topology Change - 0
Restricted Role is disabled. Restricted TCN is disabled. bpdu-transmit
enabled
bpdu-receive enabled
Multiple Instance:
Your Product# show spanning-tree detail switch default
Switch default
MST00 is executing the mstp compatible Multiple Spanning
Tree Protocol
Bridge Identifier has Priority 32768, Address
00:51:02:03:04:05
Configured Max age 20 sec 0 cs, Forward delay 15 sec 0 cs
Configured Hello Time 2 sec 0 cs
Dynamic Path Cost Disabled
Flush Interval 0 centi-sec, Flush Invocations 1
Flush Indication threshold 0
We are root of the spanning tree
Current Root has priority 32768, address
00:51:02:03:04:05
cost of root path is 0
Number of Topology Changes 1, Time since topology Change
82 seconds ago
Transmit Hold-Count 3
Root Times: Max age 20 sec 0 cs Forward delay 15 sec 0 cs
Port 1 [Gi0/1] of MST00 is Designated, Forwarding
Gi0/1 is operating in the MSTP Mode
Port path cost 200000, Port priority 128,
Port Identifier 128.1. Port HelloTime 2 secs 0 cs, Timers: Hello - 0,
Forward Delay - 0, Topology Change - 0
Designated root has priority 32768, address
00:51:02:03:04:05
Designated Bridge has priority 32768, address
00:51:02:03:04:05
Designated Port Id is 128.1, Designated pathcost is 0
Operational Forward delay 15 sec 0 cs, Max age 20 sec 0 cs

Number of Transitions to forwarding State : 1
PortFast is disabled
Link Type is Shared
BPDUs : sent 58, recieved 0
Restricted Role is disabled. Restricted TCN is disabled.
```

Related Command(s)

- `shutdown` - physical/VLAN/port-channel/tunnel Interface - Disables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.
- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree` - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree compatibility` - Sets the STP compatibility version in the switch for all ports.
- `spanning-tree timers` - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- `spanning-tree transmit hold-count` - Sets the transmit hold-count value for the switch.
- `clear spanning-tree counters` - Deletes all bridge and port level spanning tree statistics information.
- `spanning-tree pathcost dynamic` - Enables dynamic pathcost calculation feature in the switch.
- `spanning-tree priority` - Configures the priority value that is assigned to the switch.
- `spanning-tree – Properties of an interface` - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- `spanning-tree restricted-role` - Enables the restricted role feature for a port.
- `spanning-tree restricted-tcn` - Enables the topology change guard / restricted TCN feature on a port.
- `spanning-tree layer2-gateway-port` - Configures a port to operate as a L2GP.
- `spanning-tree bpdu-receive` - Configures the processing status of the BPDUs received in a port.
- `spanning-tree bpdu-transmit` - Configures the BPDU transmission status of a port.
- `spanning-tree loop-guard` - Enables the loop guard feature in a port.
- `spanning-tree – Pseudoroot configuration` - Configures the pseudoroot related information for a port set as L2GP.
- `spanning-tree mst- Properties of an interface for MSTP` - Configures the port related spanning tree information for a specified MSTI.
- `spanning-tree mst hello-time` - Configures the hello time for an interface that is enabled.
- `spanning-tree vlan` - Configures spanning tree related information on a per VLAN basis.
- `spanning-tree vlan status` - Configures the status of PVRST on a port for the specified VLAN.
- `spanning-tree vlan port-priority` - Configures the priority of a port for the specified VLAN.
- `spanning-tree vlan cost` - Configures the cost of a port for the specified VLAN.
- `spanning-tree flush-interval` - Configures the flush interval timer value.
- `spanning-tree flush-indication-threshold` - Configures the flush indication threshold value for a specific instance.

show spanning-tree active

Command Objective This command displays spanning tree related information available in the switch for the current STP enabled in the switch.

The information contains priority, address and timer details for root and bridge, status of dynamic pathcost calculation feature, status of spanning tree function, STP compatibility version used, configured spanning tree Mode, bridge and port level spanning tree statistics information, and details of ports enabled in the switch. The port details contain port ID, port role, port state, port cost, port priority and link type.

Syntax **show spanning-tree active [detail] [switch <context_name>]**

Parameter Description

- `detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch. The information contains status of spanning tree operation, current selected spanning Mode, current spanning tree compatibility version, bridge and root priority, bridge and root addresses, port path cost, port priority, port timers, bridge and port level spanning tree statistics information, transmit hold-count value, link-type, and status of L2GP, loop guard, BPDU receive, BPDU transmit, restricted TCN, restricted role and portfast features.
- `switch <context_name>` - Displays spanning tree related information available in the switch, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Note: This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

Single Instance:

```
Your Product# show spanning-tree active
Root Id    Priority 32768
Address    00:01:02:03:04:01
Cost         200000
Port         1 [Gi0/1]
Max age 20 sec 0 cs, forward delay 15 sec 0 cs
Hello Time 2 sec 0 cs
MST00
Spanning tree Protocol has been enabled
MST00 is executing the mstp compatible Multiple Spanning
Tree Protocol
Bridge Id Priority 32768
Address 00:02:02:03:04:01
Max age 20 sec 0 cs, forward delay 15 sec 0 cs
Hello Time 2 sec 0 cs
Dynamic Path Cost is Disabled
Name       Role     State        Cost         Prio  Type
----       ----     -----        ----         ----  -----
```

```
Gi0/1       Root      Forwarding    200000       128    SharedLan
```

Multiple Instance:

```
Your Product# show spanning-tree active switch default
Switch default
Root Id    Priority 32768
Address    00:51:02:03:04:05
Cost          0
Port          0 [0]
This bridge is the root
Max age 20 sec 0 cs, forward delay 15 sec 0 cs
Hello Time 2 sec 0 cs
MST00
MST00 is executing the mstp compatible Multiple Spanning
Tree Protocol
Bridge Id  Priority 32768
Address 00:51:02:03:04:05
Max age 20 sec 0 cs, forward delay 15 sec 0 cs
Hello Time 2 sec 0 cs
Name       Role            State         Cost          Prio   Type
-------    -------         --------      -------       -------   ----------
Gi0/1      Designated      Forwarding    200000        128    SharedLan
```

Related Command(s)

- `shutdown` - physical/VLAN/port-channel/tunnel Interface - Disables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.
- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree` - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree compatibility` - Sets the STP compatibility version in the switch for all ports.
- `spanning-tree timers` - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- `spanning-tree transmit hold-count` - Sets the transmit hold-count value for the switch.
- `clear spanning-tree counters` - Deletes all bridge and port level spanning tree statistics information.
- `spanning-tree pathcost dynamic` - Enables dynamic pathcost calculation feature in the switch.
- `spanning-tree priority` - Configures the priority value that is assigned to the switch.
- `spanning-tree - Properties of an interface` - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- `spanning-tree restricted-role` - Enables the restricted role feature for a port.
- `spanning-tree restricted-tcn` - Enables the topology change guard / restricted TCN feature on a port.
- `spanning-tree layer2-gateway-port` - Configures a port to operate as a L2GP.

- `spanning-tree bpdu-receive` - Configures the processing status of the BPDUs received in a port.
- `spanning-tree bpdu-transmit` - Configures the BPDU transmission status of a port.
- `spanning-tree loop-guard` - Enables the loop guard feature in a port.
- `spanning-tree – Pseudoroot configuration` - Configures the pseudoroot related information for a port set as L2GP.
- `spanning-tree mst- Properties of an interface for MSTP` - Configures the port related spanning tree information for a specified MSTI.
- `spanning-tree vlan` - Configures spanning tree related information on a per VLAN basis.
- `spanning-tree vlan status` - Configures the status of PVRST on a port for the specified VLAN.
- `spanning-tree vlan port-priority` - Configures the priority of a port for the specified VLAN.
- `spanning-tree vlan cost` - Configures the cost of a port for the specified VLAN.

show spanning-tree interface

Command Objective This command displays the port related spanning tree information for the specified interface.

The information contains port ID, port role, port state, port cost, port priority and link type. The generic command cannot be executed without any option in the PVRST Mode.

Syntax **show spanning-tree interface <interface-type> <interface- id> [{ cost | priority | portfast | rootcost | restricted- role | restricted-tcn | state | stats | detail }]**

Parameter Description

- `<interface-type>` - Displays the port related spanning tree information for the specified type of interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Displays the port related spanning tree information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For example: 1 represents port-channel ID.
- `cost` - Displays the cost of the port or instances assigned to that port. This option cannot be

executed in the PVRST Mode.

- `priority` - Displays the priority of the port or instances assigned to that port. This option cannot be executed in the PVRST Mode.
- `portfast` - Displays the status of the portfast feature for the port or instances assigned to that port.
- `rootcost` - Displays the root cost of the port or instances assigned to that port. The root cost defines the pathcost to reach the root bridge. This option cannot be executed in the PVRST Mode.
- `restricted-role` - Displays the status of the restricted role feature for the port. This option cannot be executed in the PVRST Mode.
- `restricted-tcn` - Displays the status of the restricted TCN feature for the port. This option cannot be executed in the PVRST Mode.
- `state` - Displays the state of the port. This option cannot be executed in the PVRST Mode.
- `stats` - Displays the port level spanning tree statistics information. This option cannot be executed in the PVRST Mode.
- `detail` - Displays detailed spanning tree related information for the port. The information contains current selected spanning Mode, bridge and root priority, bridge and root addresses, port path cost, port priority, port timers, bridge and port level spanning tree statistics information, link-type, and status of L2GP, loop guard, BPDU receive, BPDU transmit, restricted TCN, restricted role and portfast features. This option cannot be executed in the PVRST Mode.

Mode Privileged EXEC Mode

Note: This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

Single Instance:

```
Your Product# show spanning-tree interface gigabitethernet
0/1
Instance   Role     State        Cost         Prio         Type
--------   ----     -----        ----         ----         ----
MST00         Root  Forwarding   200000       128.1        SharedLan
Your Product# show spanning-tree interface gigabitethernet
0/1 cost
Port cost is 200000
Your Product# show spanning-tree interface gigabitethernet
0/1 priority
Port Priority is 128
Your Product# show spanning-tree interface gigabitethernet
0/1 portfast
PortFast is disabled
Your Product# show spanning-tree interface gigabitethernet
0/1 rootcost
Root Cost is 200000
Your Product# show spanning-tree interface gigabitethernet
```

```
0/1 state
Your Product# show spanning-tree interface gigabitethernet
0/1 stats
Statistics for Port Gi0/1
Number of Transitions to forwarding State : 1
Number of RSTP BPDU Count received       : 1692
Number of Config BPDU Count received     : 9

Number of TCN BPDU Count received        : 0
Number of RSTP BPDU Count Transmitted    : 735
Number of Config BPDU Count Transmitted  : 11
Number of TCN BPDU Count Transmitted     : 0
Number of Invalid BPDU Count Transmitted : 0
Port Protocol Migration Count            : 1
Your Product# show spanning-tree interface gigabitethernet
0/1 detail
Port 1 [Gi0/1] is Designated, Forwarding
Port PathCost 200000, Port Priority 128, Port Identifier
128.1
Designated Root has priority 32768, address
00:01:02:03:04:01
Designated Bridge has priority 32768, address
00:01:02:03:04:01
Designated Port Id is 128.1, Designated PathCost 0
No of Transitions to forwarding State :2
PortFast is enabled
Link Type is Shared
BPDUs : sent 1780 , recieved 254
Timers: Hello - 0, Forward Delay - 0, Topology Change - 0
Restricted Role is disabled. Restricted TCN is disabled. bpdu-transmit
enabled
bpdu-receive enabled
Your Product# show spanning-tree interface fast 0/1 restricted-role
Restricted Role is Disabled
Your Product# show spanning-tree interface fast 0/1 restricted-tcn
Restricted TCN is Disabled
```

Multiple Instance:

```
Your Product# show spanning-tree interface gigabitethernet
0/1
Switch - default
Role         State         Cost          Prio Type
----         -----         ----          ---- ----
Root         Forwarding    200000        128 SharedLan
Your Product# show spanning-tree interface gigabitethernet
0/1 cost
Port cost is 200000
Switch - default
Your Product# show spanning-tree interface gigabitethernet
0/1 priority
Switch – default
Port Priority is 128
Your Product# show spanning-tree interface gigabitethernet
0/1 portfast Switch – default PortFast is disabled
Your Product# show spanning-tree interface gigabitethernet
```

```
0/1 rootcost
Switch - default
Root Cost is 200000
Your Product# show spanning-tree interface gigabitethernet
0/1 state
Switch - default
Forwarding
Your Product# show spanning-tree interface gigabitethernet
0/1 stats
Switch - default
Statistics for Port Gi0/1
Number of Transitions to forwarding State : 1
Number of RSTP BPDU Count received       : 1692
Number of Config BPDU Count received     : 9
Number of TCN BPDU Count received        : 0
Number of RSTP BPDU Count Transmitted    : 735
Number of Config BPDU Count Transmitted  : 11
Number of TCN BPDU Count Transmitted     : 0
Number of Invalid BPDU Count Transmitted : 0
Port Protocol Migration Count            : 1
Your Product# show spanning-tree interface gigabitethernet
0/1 detail
Switch - default
Port 1 [Gi0/1] is Root     , Forwarding
Port PathCost 200000, Port Priority 128, Port Identifier
128.1
Designated Root has priority 8192, address
00:01:02:03:04:21
Designated Bridge has priority 8192, address
00:01:02:03:04:21
Designated Port Id is 128.1, Designated PathCost 0
No of Transitions to forwarding State :1
PortFast is disabled
Link Type is Shared
BPDUs : sent 735 , recieved 1729
Your Product# show spanning-tree interface fast 0/1 restricted-role
Switch - default
Restricted Role is Disabled
Your Product# show spanning-tree interface fast 0/1 restricted-tcn
Switch - default
Restricted TCN is Disabled
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree` - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree timers` - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- `clear spanning-tree counters` - Deletes all bridge and port level spanning tree statistics

information.

- `spanning-tree priority` - Configures the priority value that is assigned to the switch.
- `spanning-tree - Properties of an interface` - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- `spanning-tree restricted-role` - Enables the restricted role feature for a port.
- `spanning-tree restricted-tcn` - Enables the topology change guard / restricted TCN feature on a port.
- `spanning-tree layer2-gateway-port` - Configures a port to operate as a L2GP.
- `spanning-tree bpdu-receive` - Configures the processing status of the BPDUs received in a port.
- `spanning-tree bpdu-transmit` - Configures the BPDU transmission status of a port.
- `spanning-tree loop-guard` - Enables the loop guard feature in a port.
- `spanning-tree - Pseudoroot configuration` - Configures the pseudoroot related information for a port set as L2GP.
- `clear spanning-tree detected protocols` - Restarts the protocol migration process on all interfaces in the switch and forces renegotiation with the neighboring switches.
- `spanning-tree mst- Properties of an interface for MSTP` - Configures the port related spanning tree information for a specified MSTI.
- `spanning-tree mst hello-time` - Configures the hello time for an interface that is enabled.
- `spanning-tree bpduguard` - Configures the status of BPDU guard feature in an interface.

show spanning-tree root

Command Objective This command displays the spanning tree root information. The information contain root ID, root path cost, maximum age time, forward delay time and root port, for the RSTP. The information also contains the instance ID for MSTP.

Syntax **show spanning-tree root [{ address | cost | forward-time | id | max-age | port | priority | detail }] [switch <context_name>]**

Parameter Description

- `address` - Displays the MAC address of the root bridge.
- `cost` - Displays the cost of the root bridge.
- `forward-time` - Displays the forward delay time of the root bridge.
- `id` - Displays the ID of the root bridge.
- `max-age` - Displays the maximum age time of the root bridge.
- `port` - Displays the ID of the root port.
- `priority` - Displays the priority of the root bridge.
- `detail` - Displays the root priority, root address, root cost, root port, forward delay time and maximum age time.
- `switch <context_name>` - Displays spanning tree root information, for the specified context.

This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Note: This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of Spanning Tree Mode should be set, if the functionality is already shutdown. This configuration is not supported in PVRST Mode.

Example

Single Instance:

```
Your Product# show spanning-tree root
Root ID                RootCost MaxAge FwdDly RootPort
-------                -------- ------ ------ --------
80:00:00:01:02:03:04:11 0   20 sec 0 cs 15 sec 0 cs 0
Your Product# show spanning-tree root address
Root Bridge Address is 00:01:02:03:04:11
Your Product# show spanning-tree root cost
Root Cost is 0
Your Product# show spanning-tree root  forward-time
Forward delay is 15 sec 0 cs
Your Product# show spanning-tree root id
Root Bridge Id is 80:00:00:01:02:03:04:11
Your Product# show spanning-tree root max-age
Root MaxAge is 20 secs 0 cs
Your Product# show spanning-tree root port
Root Port is 0
Your Product# show spanning-tree root priorit
Root Priority is 32768
Your Product# show spanning-tree root detail
We are the root of the Spanning Tree
Root Id    Priority  32768
Address   00:01:02:03:04:11
Cost      0
Port      0
Max Age 20 sec 0 cs, Forward Delay 15 sec 0 cs
```

Multiple Instance:

```
Your Product# show spanning-tree root
Switch - default
Instance Root ID        RootCost MaxAge FwdDly RootPort
------------- ------------        ------------- ---------- ---------- ------------- MST00
80:00:00:01:02:03:04:01 0 20 sec 0 cs 15 sec 0 cs 0
Switch - cust1
Instance Root ID         RootCost MaxAge FwdDly RootPort
------------- ------------     ------------- ---------- ---------- ------------- MST00
00:00:00:01:02:03:04:04 200000 20 sec 0 cs 15 sec 0
cs   Gi0/2
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree timers` - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- `spanning-tree priority` - Configures the priority value that is assigned to the switch.
- `spanning-tree` - Properties of an interface - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- `spanning-tree mst hello-time` - Configures the hello time for an interface that is enabled.

show spanning-tree bridge

Command Objective This command displays the spanning tree bridge information. The information contain bridge ID, hello time, maximum age time, forward delay time and protocol enabled, for the RSTP. The information also contains the instance ID for MSTP.

Syntax **show spanning-tree bridge [{ address | forward-time | hello-time | id | max-age | protocol | priority | detail}] [switch <context_name>]**

Parameter Description

- `address` - Displays the MAC address of the bridge.
- `forward-time` - Displays the forward delay time of the bridge.
- `hello-time` - Displays the hello time of the bridge.
- `id` - Displays the ID of the bridge.
- `max-age` - Displays the maximum age time of the bridge.
- `protocol` - Displays the protocol currently enabled in the bridge.
- `priority` - Displays the priority of the bridge.
- `detail` - Displays the priority, address, maximum age time and forward delay time for the bridge.
- `switch` - Displays spanning tree bridge information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

`**Note:** This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.`

`This configuration is not supported in PVRST Mode.`

Example

Single Instance:

```
Your Product# show spanning-tree bridge address
Bridge Address is 00:01:02:03:04:21
Your Product# show spanning-tree bridge forward-time
Bridge Forward delay is 15 sec
Your Product# show spanning-tree bridge
Bridge ID               HelloTime MaxAge FwdDly Protocol
---------------         --------- ---------- ---------- -------------
80:00:00:01:02:03:04:21 2 s 0 cs 20 s 0 cs 15 s 0 cs rstp
Your Product# show spanning-tree bridge hello-time
Bridge Hello Time is 2 sec 0 cs
Your Product# show spanning-tree bridge id
Bridge ID is 80:00:00:01:02:03:04:21
Your Product# show spanning-tree bridge max-age
Bridge Max Age is 20 sec 0 cs
Your Product# show spanning-tree bridge protocol
Bridge Protocol Running is RSTP

Your Product# show spanning-tree bridge priority
Bridge Priority is 32768
Your Product# show spanning-tree bridge detail
Bridge Id    Priority 32768
Address 00:05:02:03:04:01
Max age is 20 sec 0 cs, forward delay is 15
sec 0 cs
```

Multiple Instance:

```
Your Product# show spanning-tree bridge
Switch - default
MST Instance Bridge ID          MaxAge FwdDly Protocol
-------------------- ---------------          ---------- ---------- ------------- MST00 0
:00:00:01:02:03:04:01 20 s 0 cs 15 s 0 cs mstp Switch - cust1
MST Instance Bridge ID           MaxAge FwdDly Protocol
-------------------- ---------------            ---------- ---------- ------------- MST00   0
:00:00:01:02:03:04:02 20 s 0 cs 15 s 0 cs mstp
Your Product# show spanning-tree bridge address
Switch - default
MST00    00:01:02:03:04:01
Switch - cust1
MST00    00:01:02:03:04:0
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree` - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree timers` - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- `spanning-tree priority` - Configures the priority value that is assigned to the switch.
- `spanning-tree mst hello-time` - Configures the hello time for an interface that is enabled.

show spanning-tree – layer 2 gateway port

Command Objective This command displays spanning tree information for all L2GPs enabled in the switch. The information contains pseudoroot priority, pseudo root MAC address and state of the L2GP.

Syntax **show spanning-tree [interface <interface-type> <interface- id>] layer2-gateway-port [switch <context_name>]**

Parameter Description

- `<interface-type>` - Displays L2GP related spanning tree information for the specified type of interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Displays L2GP related spanning tree information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that the slot number is 0 andport number is 1. Only port-channel ID is provided, for interface type port-channel. For example: 1 represents port-channel ID.
- `switch <context_name>` - Displays L2GP related spanning tree information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Note: This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Example

```
Your Product# show spanning-tree interface gigabitethernet 0/1 layer2-
gateway-port switch default
Switch default
Port Gi0/1
           PseudoRootId
Instance   Priority MacAddress          State
```

```
---------------------------------------------  -------------------        -----------------------------------  -------------------
                           MST00          4096          00:00:11:22:33:44    Forwarding
                           MST01          8192          00:00:12:34:45:55    Forwarding
                           MST02          4096          00:00:12:34:45:5a    Forwarding
```

Related Command(s)

- `shutdown - physical/VLAN/port-channel/tunnel Interface` - Disables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.
- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the typeof spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree layer2-gateway-port` – Configures a port to operate as a L2GP.
- `spanning-tree – Pseudoroot configuration` - Configures the pseudoroot related information for a port set as L2GP.

show customer spanning-tree

Command Objective This command displays the detailed customer spanning tree information.

Syntax **show customer spanning-tree [cep interface <interface- type> <interface-number>] [{ detail [active] | active [detail] }]**

Parameter Description

- `cep interface<interface-type> <interface-number>` - Displays the Customer Edge Port interface details. The details to be provided are:
  - `<interface-type>` - Displays the customer spanning tree related information for the CEP type of interface. The interface can be:
  - `fastethernet` – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `internal-lan` –Internal LAN created on a bridge per IEEE 802.1ap.
  - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
  - `<interface-number>` - Displays the customer spanning tree related information for the CEP interface number. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only internal-lan and port- channel ID is

provided, for interface types internal-lan and port- channel. For example: 1 represents internal-lan and port-channel ID.

- `detail` - Displays in detail about the port and bridge. This includes designated Bridge details, designated port details, timer values, root bridge and so on.
- `active` - Displays the Bridge and details of the active (active ports are those ports that are participating in the spanning-tree) ports

Mode Privileged EXEC Mode

Note: The port must be configured as CEP. This feature is not available on some SMIS switch models.

Example

Single Instance:

```
Your Product# show customer spanning-tree cep interface fast 0/1
Port [Gi0/1]
We are the root of the Spanning Tree
Root Id    Priority  65535
Address   00:01:02:03:04:01
Cost      0
Root Ports
Hello Time 2 Sec 0 cs, Max Age 20 Sec 0 cs,
Forward Delay 15 Sec 0 cs
Customer Spanning Tree Enabled Protocol RSTP
Bridge Id Priority 65535
Address 00:01:02:03:04:01
Hello Time 2 Sec 0 cs, Max Age 20 Sec 0 cs,
Forward Delay 15 Sec 0 cs
Name     Role     State       Cost    Prio  Type
-------   -------  -------     -------  ------  ----------
PEP-Service: 2 Designated Forwarding 128   32 SharedLan
CEP-Gi0/1    Designated Forwarding 200000 32 SharedLan
Your Product# show customer spanning-tree
Port [Gi0/1]
We are the root of the Spanning Tree
Root Id    Priority  65535
Address   00:01:02:03:04:01
Cost      0
Root Ports
Hello Time 2 Sec, Max Age 0 Sec, Forward
Delay 0 Sec
Customer Spanning Tree Enabled Protocol RSTP
Bridge Id    Priority 65535
Address 00:01:02:03:04:01
Hello Time 2 Sec 0 cs, Max Age 20 Sec 0 cs,
Forward Delay 15 Sec 0 cs
Name     Role   State       Cost    Prio  Type
-------  -------  -------     -------  -------  ----------
PEP-Service: 2 Designated  Forwarding 128 32 SharedLan
CEP-Gi0/1 Designated  Forwarding 200000 32 SharedLan
```

Multiple Instance:

```
Your Product# show customer spanning-tree
Switch default
Port [Gi0/1]
We are the root of the Spanning Tree
Root Id       Priority  65535
Address    00:01:02:03:04:01
Cost       0
Root Ports
Hello Time 2 Sec 0 cs, Max Age 20 Sec 0 cs,
Forward Delay 15 Sec 0 cs
Customer Spanning Tree Enabled Protocol RSTP
Bridge Id Priority 65535
Address 00:01:02:03:04:01
Hello Time 2 Sec 0 cs, Max Age 20 Sec 0 cs,
Forward Delay 15 Sec 0 cs
Name      Role        State       Cost     Prio  Type
-------   -------     --------    -------  ------- ----------
PEP-Service: 2 Designated Forwarding 128  32 SharedLan
CEP-Gi0/1      Designated Forwarding 200000 32 SharedLan
Your Product# show customer spanning-tree cep interface fastethernet 0/1
Switch default
Port [Gi0/1]
We are the root of the Spanning Tree
Root Id       Priority  65535
Address    00:01:02:03:04:01
Cost       0
Root Ports
Hello Time 2 Sec 0 cs, Max Age 20 Sec 0 cs,
Forward Delay 15 Sec 0 cs
Customer Spanning Tree Enabled Protocol RSTP
Bridge Id     Priority 65535
Address 00:01:02:03:04:01
Hello Time 2 Sec 0 cs, Max Age 20 Sec 0 cs,
Forward Delay 15 Sec 0 cs
Name        Role    State     Cost    Prio  Type
-------     ------- --------  ------- ------- ----------
PEP-Service: 2 Designated Forwarding 128  32 SharedLan
CEP-Gi0/1      Designated Forwarding 200000 32 SharedLan
```

Related Command(s) `show customer spanning-tree` – Displays the detailed customer spanning information

spanning-tree forwarddelay optimization alternate-role

Command Objective This command enables or disables the optimization for spanning-tree related protocol during transition from alternate to designated port role.

When role translation takes place from alternate to designated, the value with which forward-delay timer started is controlled by executing this command.

Syntax **spanning-tree forwarddelay optimization alternate-role {enabled | disabled}**

Parameter Description

- `enabled` - Enables optimization for spanning-tree related protocol in alternate port role transition.
- `disabled` - Disables the optimization for spanning-tree related protocol in alternate port role transition.

Mode Global Configuration Mode

Note: This command executes only if the RSTP is enabled.

Default enabled

Example

```
Your Product(config)# spanning-tree forwarddelay optimization alternate-
role enabled
```

Related Command(s) `spanning-tree mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch. The current selected type of spanning tree is enabled and the existing spanning tree type is disabled in the switch.

17 MSTP

Aricent MSTP is a portable implementation of the IEEE 802.1s standard. It is used to configure spanning tree on per VLAN basis or multiple VLANs per spanning tree. It allows you to build several MST over VLAN trunks, and group or associate VLANs to spanning tree instances, so the topology of one instance is independent of the other instance. It provides multiple forwarding paths for data traffic and enables load balancing. It improves the overall network fault tolerance, as failure in one instance does not affect the other instances.

This section describes all the commands for MSTP Configurations. The list of commands for the configuration of MSTP is as follows:

- spanning-tree mst max-hops
- spanning-tree mst configuration
- spanning-tree mst max-instance
- spanning-tree mst root
- spanning-tree mst forward-time
- spanning-tree mst max-age
- name
- revision
- instance
- spanning-tree mst- Properties of an interface for MSTP

- spanning-tree mst hello-time
- show spanning-tree mst - CIST or specified mst Instance
- show spanning-tree mst configuration
- show spanning-tree mst - Port Specific Configuration
- spanning-tree flush-interval
- spanning-tree flush-indication-threshold

spanning-tree mst max-hops

Command Objective This command configures the maximum number of hops permitted in the MSTP. This value ranges between 6 and 40.

The number of hops represents the maximum number of switches that a packet can cross before it is dropped. The switch uses this value to avoid infinite looping of the packets, if it is elected as the root switch in the topology.

The root switch always transmits a BPDU with the maximum hop count value. The receiving switch decrements the value by one and propagates the BPDU with modified hop count value. The BPDU is discarded and the information held is aged out, when the count reaches 0.

The no form of this command resets the maximum number of hops to its default value.

Syntax **spanning-tree mst max-hops <value(6-40)>**

no spanning-tree mst max-hops

Mode Global Configuration Mode

Default 20

Note: This command can be executed successfully, only if the spanning tree functionality is started in the switch. The type of spanning tree Mode should be set as mst.

Example

```
Your Product(config)#spanning-tree mst max-hops 10
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree mst` - CIST or specified mst Instance -- Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst` - Port Specific Configuration - Displays multiple spanning tree port specific information for the specified port.

spanning-tree mst configuration

Command Objective This command enters into MSTP configuration Mode, where instance specific and MST region configuration can be done.

Syntax **spanning-tree mst configuration**

Mode Global Configuration Mode

This command can be executed successfully, only if the spanning tree functionality is started and enabled in the switch. The type of spanning tree Mode should be set as mst.

Example Your Product(config)#spanning-tree mst configuration

Related Command(s)

- `shutdown spanning-tree` – Shuts down spanning tree functionality in the switch.
- `spanning-tree mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.

spanning-tree mst max-instance

Command Objective This command configures the maximum number of active MSTIs that can be created. This value ranges between 1 and 64.

This configuration allows you to limit the number of spanning tree instances to be allowed in the switch. This does not count the special MSTID such as PTETID, used to identify the VIDs which are used by ESPs.

The no form of this command resets maximum MSTP instance value to its default value.

Syntax **spanning-tree mst max-instance <short(1-64)>**

no spanning-tree mst max-instance

Mode Global Configuration Mode

Default 64

This command can be executed successfully, only if the spanning tree functionality is started and enabled in the switch. The type of spanning tree Mode should be set as mst.

Example

```
Your Product(config)# spanning-tree mst max-instance 40
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `instance` - Creates an MST instance and maps it to VLANs.

spanning-tree mst root

Command Objective This command enables BPDU (Bridge Protocol Data Unit) transmission and reception on the interface. This command is a standardized implementation of the existing command; spanning-tree priority. It operates similar to the existing command.

The no form of the command disables BPDU transmission and reception on the interface.

Syntax **spanning-tree mst {instance-id <instance-id(1-64)>} root {primary | secondary}**

no spanning-tree mst {instance-id <instance-id(1-64)>} root

Parameter Description

- `instance-id <instance-id(1-64)>` - Configures the ID of MSTP instance already created in the switch. This value ranges between 1 and 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs. This option is applicable, only if the spanning tree Mode is set as mst.
- `primary` - Sets high enough priority (low value) for the switch so that the switch can be made as the bridge root of the spanning-tree instance. The priority value is set as 24576.
- `secondary` - Sets the switch as a secondary root, if the primary root fails. The priority value is set as 28672.

Mode Global Configuration Mode

Note: This command executes only if

- instance is created
- spanning tree Mode is set as mst.

Example

```
Your Product(config)# spanning-tree mst instance-id 1 root secondary
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree mst configuration` – Enters into MSTP configuration Mode, where instance specific and MST region configuration can be done.
- `instance` - Creates an MST instance and maps it to VLANs.
- `show spanning-tree detail` - Displays detailed spanning tree information
- `show spanning-tree active` - Displays spanning tree information of active ports

spanning-tree mst forward-time

Command Objective This command configures the forward timer of the spanning tree and the no form of the command sets the forward timer to the default value. The forward timer controls the speed at which a port changes its spanning tree state from Blocking state to Forwarding state. The timer value ranges between 4 and 30 seconds.

Notes:

1. This command is currently not supported.
2. The values configured for the spanning tree forward timers should satisfy the following conditions: 2* (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1)
3. This command is a standardized implementation of the existing command; spanning-tree timers. It operates similar to the existing command.

Syntax **spanning-tree mst forward-time <seconds(4-30)>**

no spanning-tree mst forward-time

Mode Global Configuration Mode

Default forward-time - 15 secs

Notes:

1. The STP forward timers can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.
2. This spanning tree timer's configuration is not supported in PVRST Mode.

Example

```
Your Product(config)# spanning-tree mst forward-time 4
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- spanning-tree Mode - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree` - Summary, Blockedports, Pathcost, redundancy - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree interface` detail - Displays detailed spanning tree related information for the specified port.
- `show spanning-tree root` - Displays the spanning tree root information.
- `show spanning-tree bridge` - Displays the spanning tree bridge information.
- `show spanning-tree mst` - CIST or specified mst Instance - Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst` - Port Specific Configuration - Displays multiple spanning tree port specific information for the specified port.

spanning-tree mst max-age

Command Objective This command configures the max-age timer of the spanning tree. The max- age timer denotes the time (in seconds) after which the spanning tree protocol information learnt from the network on any port will be discarded. The timer value ranges between 6 and 40 seconds.

The no form of the command sets the max-age timer to the default value

Notes:

1. Max-age timer can be configured in centi seconds through SNMP
2. The values configured for the spanning tree forward timers should satisfy the following conditions:

- 2* (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1)
- This command is a standardized implementation of the existing command; spanning-tree timers. It operates similar to the existing command.

Syntax **spanning-tree mst max-age <seconds(6-40)>**

no spanning-tree mst max-age

Mode Global Configuration Mode

Default max-age - 20 secs

Notes:

1. The STP forward timers can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.
2. This spanning tree timer's configuration is not supported in PVRST Mode.

Example

```
Your Product(config)# spanning-tree mst max-age 7
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree` - Summary, Blockedports, Pathcost, redundancy - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- show spanning-tree detail - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- show spanning-tree active - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- show spanning-tree interface detail - Displays detailed spanning tree related information for the specified port.

- show spanning-tree root - Displays the spanning tree root information.
- show spanning-tree bridge - Displays the spanning tree bridge information.
- show spanning-tree mst - CIST or specified mst Instance - Displays multiple spanning tree information for all MSTIs in the switch.
- show spanning-tree mst - Port Specific Configuration - Displays multiple spanning tree port specific information for the specified port.

name

Command Objective This command configures the name for the MST region.

The name is unique and used to identify the specific MST region. Each MST region contains multiple spanning tree instances and runs special instance of spanning tree known as IST to disseminate STP topology information for other STP instances.

The no form of this command resets the name to its default value.

Syntax **name <string(32)>**

Mode MSTP Configuration Mode

Default Same as that of the base MAC address of the switch.

Example

```
Your Product(config-mst)#name regionone
```

Related Command(s) `show spanning-tree mst configuration` - Displays multiple spanning tree instance related information.

revision

Command Objective This command configures the revision number for the MST region. This value ranges between 0 and 65535.

The no form of this command resets the revision number to its default value.

Syntax **revision <value(0-65535)>**

no revision

Mode MSTP Configuration Mode

Default 0

Example

```
Your Product(config-mst)#revision 100
```

Related Command(s) `show spanning-tree mst configuration` - Displays multiple spanning tree instance related information.

instance

Command Objective This command creates an MST instance and maps it to VLANs.

The no form of this command deletes the instance / unmaps specific VLANs from the MST instance.

Syntax **instance <instance-id(1-64|4094)> vlan <vlan-range>**

no instance <instance-id (1-64)> [vlan <vlan-range>]

Parameter Description

- `<instance-id(1-64|4094)>` - Configures the ID of MSTP instance to be created / deleted and mapped with / unmapped from VLAN. This value ranges between 1 to 64. The special value 4094 can be used in the switch that supports PBB-TE. Except vlan instance mapping, other commands for stp configurations will not be applicable in this Mode.This special value represents PTETID that identifies VID used by ESPs.
- `vlan <vlan-range>` - Configures a VLAN ID or list of VLAN IDs that should be mapped with / unmapped from the specified MST instance. This value is a string whose maximum size is 9. For example, the value is provided as 4000-4010 to represent the list of VLANs IDs from 4000 to 4010.

Mode MSTP configuration Mode

Default Instance 0 is created and mapped with all VLANs (1-4094).

Example Your Product(config-mst)#instance 2 vlan 2

Related Command(s)

- `spanning-tree priority` - Configures the priority value that is assigned to the switch.
- `spanning-tree` – Pseudoroot configuration - Configures the pseudoroot related information for a port set as L2GP.
- `spanning-tree mst max-instance` - Configures the maximum number of active MSTIs that can be created.
- `spanning-tree mst- Properties of an interface for MSTP -` Configures the port related spanning tree information for a specified MSTI.
- `show spanning-tree mst - CIST or specified mst Instance` - Displays multiple spanning tree information for all MSTIs in the switch.
- `show spanning-tree mst configuration` - Displays multiple spanning tree instance related information.
- `show spanning-tree mst` - Port Specific Configuration - Displays multiple spanning tree port specific information for the specified port

spanning-tree mst- Properties of an interface for MSTP

Command Objective This command configures the port related spanning tree information for a specified MSTI in a port.

The no form of this command resets the spanning tree information of a port to its default value.

Syntax **spanning-tree mst <instance-id(1-64)> { cost <value(1-200000000)>| port-priority <value(0-240)> | disable }**

no spanning-tree mst <instance-id(1-64)>{cost|port- priority | disable}

Parameter Description

- `<instance-id(1-64)>` - Configures the ID of MSTP instance already created in the switch.This value ranges between 1 to 64.
- `cost<value(1-200000000`)> - Configures the port's path cost value that contributes to the path cost of paths containing this particular port. The paths' path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. This value ranges between 1 and 200000000. The configured path cost is used, even if the dynamic pathcost calculation feature or LAGG speed feature is enabled.
- `port-priority<value(0-240)>` - Configures the priority value assigned to the port. This value is used during port role selection process. This value ranges between 0 and 240. This value should be set in steps of 16, that is, you can set the value as 0, 16, 32, 48, and so on. The MSTP puts the interface with lowest number in forwarding state and blocks all other interfaces, if all interfaces have the same priority value.
- `disable` - Disables the spanning tree operation on the port. The port does not take part in the execution of spanning tree operation for preventing undesirable loops in the network.

Mode Interface Configuration Mode (Physical Interface Mode)

Default

- cost - 200000 for all physical ports; 199999 for port channels
- port-priority - 128
- disable - Spanning tree operation is enabled in the port.

Note: This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set as mst

Example

```
Your Product(config-if)#spanning-tree mst 2 cost 4000
Your Product(config-if)#spanning-tree mst 1 port-priority 32
Your Product(config-if)#spanning-tree mst 2 disable
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree pathcost dynamic` - Enables dynamic pathcost calculation feature in the switch.
- `instance` - Creates an MST instance and maps it to VLANs.

- `show spanning-tree` - Summary, Blockedports, Pathcost, redundancy - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.
- `show spanning-tree active` - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree interface` - Displays the port related spanning tree information for the specified interface.
- `show spanning-tree` mst - CIST or specified mst Instance - Displays multiple spanning tree information for all MSTIs in the switch.

spanning-tree mst hello-time

Command Objective This command configures the spanning tree hello time.

The no form of this command resets the hello time to its default value.

The hello time represents the time interval (in seconds) between two successive configuration BPDUs generated by the switch on the port. This value is either 1 or 2 seconds. This value is applied to all active MSTIs.

Note: Hello Time can be configured in centi seconds through SNMP

Syntax **spanning-tree mst hello-time<value(1-2)>**

no spanning-tree mst hello-time

Mode Global Configuration Mode, Interface Configuration Mode (Physical Interface Mode)

Default 2 seconds

Note: This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set as mst.

Example

```
Your Product(config-if)#spanning-tree mst hello-time 1

Your Product(config)#spanning-tree mst hello-time 1
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- spanning-tree Mode - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `show spanning-tree` - Summary, Blockedports, Pathcost, redundancy - Displays spanning tree related information available in the switch for the current STP enabled in the switch.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.

- show spanning-tree interface - Displays the port related spanning tree information for the specified interface.
- show spanning-tree root - Displays the spanning tree root information.
- show spanning-tree bridge - Displays the spanning tree bridge information.
- show spanning-tree mst - Port Specific Configuration - Displays multiple spanning tree port specific information for the specified port.

show spanning-tree mst - CIST or specified mst Instance

Command Objective This command displays multiple spanning tree information for all MSTIs in the switch.

The information contain MSTI ID, VLAN IDs mapped to the instance, bridge address and priority, root address and priority, IST root address, priority and path cost, forward delay, maximum age, maximum hop count, and port details of interfaces enabled in the switch. The port details contain interface ID, port role, port state, port cost, port priority and port link type.

Syntax **show spanning-tree mst [<instance-id(1-64|4094)>] [detail] [switch <context_name>]**

Parameter Description

- <instance-id(1-64|4094)> - Displays the multiple spanning tree information for the specified MSTI. This value ranges between 1 to 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs.
- detail - Displays the detailed multiple spanning tree information for the MSTI. This information contain MSTI ID, VLAN IDs mapped to the instance, bridge address and priority, root address and priority, IST root address, priority and path cost, forward delay, maximum age, maximum hop count, and BPDUs sent and received in the port.
- switch<context_name> - Displays multiple spanning tree bridge information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Note: This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set as mst.

Example **Single Instance:**

```
Your Product# show spanning-tree mst 1
## MST01
Vlans mapped:   2
Bridge     Address 00:01:02:03:04:11    Priority 32768
Root       Address 00:01:02:03:04:11    Priority 32768
Root       this switch for MST01
```

```
Interface Role       Sts    Cost   Prio.Nbr Type
-------------- -------       -----    -------   ------------ -------
Gi0/1 Master  Forwarding  200000   128.1  SharedLan
Your Product# show spanning-tree mst 1 detail
## MST01
Vlans mapped:   2
Bridge    Address 00:01:02:03:04:11    Priority 32768
Root      Address 00:01:02:03:04:11    Priority 32768
Root      this switch for MST01
Gi0/1 of MST01 is Master   , Forwarding
Port info  port id 128.1    priority 128  cost 200000
Designated root  address 00:01:02:03:04:11priority

32768 cost 0
Designated bridge address 00:01:02:03:04:11    priority
32768 port id 128.1
```

Multiple Instance:

```
Your Product# show spanning-tree mst 1
Switch - default
## MST01
Vlans mapped:   2
Bridge    Address 00:01:02:03:04:11    Priority 32768
Root      Address 00:01:02:03:04:11    Priority 32768
Root      this switch for MST01
Interface Role      Sts      Cost   Prio.Nbr Type
--------- ----      ---      ----   -------- ----
Gi0/1      Master  Forwarding  200000   128.1  SharedLan
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree` - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree timers` - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- `clear spanning-tree counters` - Deletes all bridge and port level spanning tree statistics information.
- `spanning-tree priority` - Configures the priority value that is assigned to the switch.
- `spanning-tree` - Properties of an interface - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- `spanning-tree layer2-gateway-port` - Configures a port to operate as a L2GP.
- `spanning-tree – Pseudoroot configuration` - Configures the pseudoroot related information for a port set as L2GP.
- `spanning-tree mst max-hops` - Configures the maximum number of hops permitted in the MST.
- `instance` - Creates an MST instance and maps it to VLANs.
- `spanning-tree mst` - Properties of an interface for MSTP - Configures the port related spanning

tree information for a specified MSTI.

- shutdown - physical/VLAN/port-channel/tunnel Interface - Disables a physical interface / VLAN interface / port-channel interface / tunnel interface.

show spanning-tree mst configuration

Command Objective This command displays multiple spanning tree instance related information. This information contains the MST region name, MST region revision, and a list containing MSTI IDs and VLAN IDs mapped to the corresponding MSTI.

Syntax **show spanning-tree mst configuration [switch <context_name>]**

Parameter Description

switch <context_name> - Displays multiple spanning tree instance related information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Note: This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set as mst.

Example **Single Instance:**

```
Your Product# show spanning-tree mst configuration
Name            [00:02:02:03:04:01] Revision       0
Instance        Vlans mapped
------------------------
0              1,3-1024,1025-2048,2049-3072,
3073-4094
1             2
-------------------------------------------------------------------------------------------------------------
```

Multiple Instance:

```
Your Product# show spanning-tree mst configuration
Switch - default
Name            [00:01:02:03:04:01] Revision       0
Instance        Vlans mapped
----------------      ------------------------------------------------------------------------------------
0              1-1024,1025-2048,2049-3072,3073-4094
-------------------------------------------------------------------------------------------------------------
Switch - cust1
Name            [00:01:02:03:04:02] Revision       0
Instance        Vlans mapped
----------------      ------------------------------------------------------------------------------------
0              1-1024,1025-2048,2049-3072,3073-4094
-------------------------------------------------------------------------------------------------------------
```

Related Command(s)

- shutdown spanning-tree - Shuts down spanning tree functionality in the switch.
- spanning-tree Mode - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- name - Configures the name for the MST region.
- revision - Configures the revision number for the MST region.
- instance - Creates an MST instance and maps it to VLANs.

show spanning-tree mst - Port Specific Configuration

Command Objective This command displays multiple spanning tree port specific information for the specified port. This information contains interface ID, edge port status, port link type, port hello time, BPDUs sent and received on the port, and instance related details. The instance details contain MSTI ID, MSTI role, MSTI status, MSTI cost and MSTI priority.

Syntax **show spanning-tree mst [<instance-id(1-64|4094)>] interface <interface-type> <interface-id> [{ stats | hello-time | detail }]**

Parameter Description

- <instance-id(1-64|4094)> - Displays the multiple spanning tree port specific information for the specified MSTI. This value ranges between 1 to 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs.
- <interface-type> - Displays the multiple spanning tree port specific information for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- <interface-id> - Displays the multiple spanning tree port specific information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that the slotnumber is 0 and port number is 1. Only port-channel ID isprovided, for interface type port-channel. For example: 1 represents port- channel ID.
- stats - Displays the number of BPDUs sent and received for the MSTIs assigned to the specified interface.
- hello-time - Displays the hello time of the MSTIs assigned to the specified interface.
- detail - Displays detailed multiple spanning tree port specific information for the specified interface. The information contains port priority, port cost, root address, priority and cost, IST address, priority and cost, bridge address, priority and cost, forward delay, maximum age, maximum

hop count, and BPDUs sent and received.

Mode Privileged EXEC Mode

Note: This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set as mst.

Example

```
Your Product# show spanning-tree mst 1 interface gigabitethernet 0/1
```

```
Switch default
Gi0/1 of MST00 is Disabled , Discarding
Edge port: no
Link type: Shared
Port Hello Timer: 2 sec 0 cs
Bpdus sent 0 , Received 0
Instance                Role          Sts          Cost          Prio.Nbr
--------                  ----        ---          ----   --------
0                         Disabled    Discarding   200000        128.1
Your Product# show spanning-tree mst 1 interface gigabitethernet 0/1 stats
MST01    Bpdus sent 2, Received 0
Your Product# show spanning-tree mst 1 interface gigabitethernet 0/1 hello-time
MST01    2 secs 0 cs
Your Product# show spanning-tree mst 1 interface gigabitethernet 0/1 detail
Gi0/1 of MST01 is Master   , Forwarding
Port info    port id 128.1      priority 128   cost
200000
Designated root address 00:01:02:03:04:11    priority
32768 cost 0
Designated bridge address 00:01:02:03:04:11    priority
32768 port id 128.1
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree` - Enables the spanning tree operation in the switch for the selected spanning tree Mode.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree timers` - Sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology.
- `clear spanning-tree counters` - Deletes all bridge and port level spanning tree statistics information.
- `spanning-tree priority` - Configures the priority value that is assigned to the switch.
- `spanning-tree` - Properties of an interface - Configures the port related spanning tree information for all kinds of STPs and creates port in STP when Automatic Port Create feature is disabled.
- `spanning-tree layer2-gateway-port` – Configures a port to operate as a L2GP.
- `spanning-tree` – Pseudoroot configuration - Configures the pseudoroot related information for a port set as L2GP.
- `spanning-tree mst max-hops` - Configures the maximum number of hops permitted in the MST.

- `instance` - Creates an MST instance and maps it to VLANs.
- `spanning-tree mst hello-time` - Configures the hello time for an interface that is enabled.

spanning-tree flush-interval

Command Objective This command configures the flush interval timer value (in centi-seconds), which controls the number of flush indications invoked from spanning-tree module per instance basis. This value ranges between 0 and 500 centi-seconds.

If the flush interval timer is set to zero, port and instance based flushing occurs(default functionality). If it is set to non-zero, instance based flushing occurs (dependent on the flush-indication-threshold value).

The no form of the command resets the flush-interval timer to the default value.

Syntax **spanning-tree flush-interval <centi-seconds (0-500)>**

no spanning-tree flush-interval

Mode Global Configuration Mode

Default flush-interval - 0 centi-secs
Note: This command executes only if the spanning tree Mode is set as mst.

Example

```
Your Product(config)# spanning-tree flush-interval 20
```

Related Command(s)

- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree flush-indication-`threshold – Sets the spanning tree flush indication threshold for a specific instance.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch.

spanning-tree flush-indication-threshold

Command Objective This command configures the flush indication threshold value for a specific instance. This indicates the number of flush indications to go before the flush- interval timer method triggers. This value ranges between 0 and 65535.

When flush indication threshold is default value and flush interval is non- default value, instance based flushing occurs during the first flush indication trigger. When the flush indication threshold value is non-default(x) and flush- interval value is non-default, port & instance based flushing is triggered until the threshold(x) is reached. Once the threshold is reached, instance based flushing is triggered & timer starts.

The no form of the command sets the flush indication threshold of the specific instance to the default value.

Syntax **spanning-tree [mst <instance-id>] flush-indication- threshold <value (0-65535)>**

no spanning-tree flush-indication-threshold

Mode Global Configuration Mode

Default flush-indication-threshold - 0

Note: This command executes only if

- the spanning tree Mode is set as mst.
- the instance is created

Example

```
Your Product(config)# spanning-tree flush-indication- threshold 2
```

Related Command(s)

- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree Mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `spanning-tree flush-interval` – Sets the spanning-tree flush interval timer value.
- `instance` - Creates an MST instance and maps it to VLANs.
- `show spanning-tree detail` - Displays detailed spanning tree related information of the switch and all ports enabled in the switch

18 LA and MLAG

LA (Link Aggregation) is a method of combining physical network links into a single logical link for increased bandwidth. LA increases the capacity and availability of the communications channel between devices (both switches and end stations) using existing Fast Ethernet and Gigabit Ethernet technology. LA also provides load balancing where the processing and communication activity is distributed across several links in a trunk, so that no single link is overwhelmed. By taking multiple LAN connections and treating them as a unified, aggregated link, practical benefits in many applications can be achieved. LA provides the following important benefits:

- Higher link availability
- Increased link capacity

Improvements are obtained using existing hardware (no upgrading to higher- capacity link technology is necessary).

The list of CLI commands for the configuration of LA is as follows:

- shutdown port-channel
- set port-channel
- channel-protocol
- lacp system-priority

- lacp system-identifier
- port-channel load-balance
- lacp port-priority
- lacp port-identifier
- channel-group
- lacp wait-time
- lacp timeout
- lacp rate
- lacp admin-key
- default port
- port-channel max-ports
- debug lacp
- debug etherchannel
- show etherchannel
- show interfaces - etherchannel
- show lacp
- mlag portal-address
- mlag portal-priority
- mlag portal-system-number
- show mlag

shutdown port-channel

Command Objective This command shuts down LA feature in the switch and releases all resources allocated to the LA feature.

The no form of the command starts and enables LA feature in the switch, and allocates required memory to the LA module. The LA feature is made available in the switch only if the LA is enabled in the switch.

LA feature allows aggregating individual point-to-point links into a port channel group, so that the capacity and availability of the communications channel between devices are increased using the existing interface technology.

Syntax **shutdown port-channel**

no shutdown port-channel

Mode Global Configuration Mode

Default LA is started in the switch, but not enabled. That is LA operational status is disabled.

Note: LA cannot be started in the switch, if the base bridge Mode is configured as transparent bridging.

Example

```
Your Product(config)# shutdown port-channel
```

Related Command(s)

- `base bridge-Mode` - Configures the base Mode (either 802.1d transparent bridge Mode or 802.1q vlan aware bridge Mode) in which the VLAN feature should operate on the switch.
- `set port-channel` - Configures the admin status of LA in the switch.
- `lacp system-priority` - Configures the LACP priority that is associated with actor's system ID.
- `lacp system-identifier` - Configures the global LACP system ID.
- `port-channel load-balance` - Configures the load balancing policy for all port channels created in the switch.
- `lacp port-priority` - Configures the LACP port priority.
- `lacp port-identifier` - Configures the LACP actor admin port ID to be filled in the LACP PDUs.
- `channel-group` - Adds the port as a member of the specified port channel that is already created in the switch.
- `lacp wait-time` - Configures the LACP wait-time for an interface.
- `lacp timeout` - Configures the LACP timeout period within which LACPDUs should be received on a port to avoid timing out of the aggregated link.
- `lacp admin-key` - Configures the LACP actor admin key and LACP Mode for a port.
- `default port` - Configures the port that should be set as default port for a port channel.
- `port-channel max-ports` - Configures the maximum number of ports that can be attached to a port channel.
- `show etherchannel` - Displays Etherchannel information for all port- channel groups created in the switch.
- `show interfaces` - etherchannel - Displays Etherchannel details for all aggregated ports and port channels.
- `show lacp` - Displays LACP counter / neighbor information for all port- channels.
- `interface-configuration and deletion` - Allows to configure interface such as out of band management, port channel, tunnel and so on.

set port-channel

Command Objective This command configures the admin status of LA in the switch. The LA feature is made available in the switch only if the LA is enabled in the switch.

LA feature allows aggregating individual point-to-point links into a port channel group, so that the capacity and availability of the communications channel between devices are increased using the existing interface technology.

Syntax **set port-channel { enable | disable }**

Parameter Description

- `enable` - Enables LA feature in the switch. Also starts the LA in the switch if the LA is shutdown.
- `disable` - Disables LA feature in the switch.

Mode Global Configuration Mode

Default disable

Example Your Product(config)# set port-channel enable

Related Command(s)

- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.
- `lacp system-priority` - Configures the LACP priority that is associated with actor's system ID.
- `lacp system-identifier` - Configures the global LACP system ID.
- `port-channel load-balance` - Configures the load balancing policy for all port channels created in the switch.
- `lacp port-priority` - Configures the LACP port priority.
- `lacp port-identifier` - Configures the LACP actor admin port ID to be filled in the LACP PDUs.
- `channel-group` - Adds the port as a member of the specified port channel that is already created in the switch.
- `lacp wait-time` - Configures the LACP wait-time for an interface.
- `lacp timeout` - Configures the LACP timeout period within which LACPDUs should be received on a port to avoid timing out of the aggregated link.
- `lacp admin-key` - Configures the LACP actor admin key and LACP Mode for a port.
- `default port` - Configures the port that should be set as default port for a port channel.
- `port-channel max-ports` - Configures the maximum number of ports that can be attached to a port channel.
- `show etherchannel` - Displays Etherchannel information for all port- channel groups created in the switch.
- `show interfaces – etherchannel` - Displays Etherchannel details for all aggregated ports and port channels.
- `show lacp` - Displays LACP counter / neighbor information for all port- channels.
- `interface-configuration and deletion` - Allows to configure interface such as out of band management, port channel, tunnel and so on

channel-protocol

Command Objective This command enables link aggregation in the switch. This command is a standardized implementation of the existing command; set port-channel. It operates similar to the existing command.

The no form of the command disables link aggregation in the switch.

Syntax **channel-protocol { lacp | pagp }**

no channel-protocol

Parameter Description

- `lacp` - Configures LACP (Link Aggregation Control Protocol) to manage channeling.
- `pagp` - Configures PAgP (Port aggregation protocol) to manage channeling. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Global Configuration Mode

Default Link aggregation is disabled

Example Your Product(config)# channel-protocol lacp

Related Command(s)

- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.
- `set port-channel` - Configures the admin status of LA in the switch
- `lacp system-priority` - Configures the LACP priority that is associated with actor's system ID.
- `lacp system-identifier` - Configures the global LACP system ID.
- `port-channel load-balance` - Configures the load balancing policy for all port channels created in the switch.
- `lacp port-priority` - Configures the LACP port priority.
- `lacp port-identifier` - Configures the LACP actor admin port ID to be filled in the LACP PDUs.
- `channel-group` - Adds the port as a member of the specified port channel that is already created in the switch.
- `lacp wait-time` - Configures the LACP wait-time for an interface.
- `lacp timeout` - Configures the LACP timeout period within which LACPDUs should be received on a port to avoid timing out of the aggregated link.
- `lacp admin-key` - Configures the LACP actor admin key and LACP Mode for a port.
- `default port` - Configures the port that should be set as default port for a port channel.
- `port-channel max-ports` - Configures the maximum number of ports that can be attached to a port channel.
- `show etherchannel` - Displays Etherchannel information for all port- channel groups created in the switch.
- `show interfaces` - etherchannel - Displays Etherchannel details for all aggregated ports and port channels.
- `show lacp` - Displays LACP counter / neighbor information for all port- channels.
- `interface-configuration and deletion` - Allows to configure interface such as out of band management, port channel, tunnel and so on.

lacp system-priority

Command Objective This command configures the LACP priority associated with actor's system ID. This priority value ranges between 0 and 65535. The switch with the lowest LACP decides the standby and active links in the LA.

The no form of the command resets the LACP priority to its default value.

Syntax **lacp system-priority <0-65535>**

no lacp system-priority

Mode Global Configuration Mode

Default 32768

Note: This command executes successfully, only if

- the LA functionality is started and enabled in the switch.
- when D-LAG status is disabled

Example

```
Your Product(config)# lacp system-priority 5
```

Related Command(s)

- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.
- `set port-channel` - Configures the admin status of LA in the switch.
- `show etherchannel` - Displays Etherchannel information for all port- channel groups created in the switch.

lacp system-identifier

Command Objective This command configures the global LACP system ID. The system ID denotes a 6-octet unicast MAC address value that is used as a unique identifier for the switch containing the aggregator.

The no form of the command resets the global LACP System ID to its default value.

Syntax **lacp system-identifier <aa:aa:aa:aa:aa:aa>**

no lacp system-identifier

Mode Global Configuration Mode

Note: This command executes successfully, only if the LA functionality is started and enabled in the switch.

Example

```
Your Product(config)#lacp system-identifier
00:01:02:03:04:05
```

Related Command(s)

- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.

- `set port-channel` - Configures the admin status of LA in the switch.

port-channel load-balance

Command Objective This command configures the load balancing policy for all port channels created in the switch.

The policy sets the rule for distributing the Ethernet traffic among the aggregated links to establish load balancing.

The no form of the command resets the load balancing policy to its default value.

Syntax **port-channel load-balance ([src-mac][dest-mac][src-dest- mac][src-ip][dest-ip][src-dest-ip][vlan-id][service- instance][mac-src-vid][mac-dest-vid][mac-src-dest- vid][dest-ip6][src-ip6][l3-protocol][dest-l4-port][src-l4- port][mpls-vc-label][mpls-tunnel-label][mpls-vc-tunnel- label])[<port-channel-index(1-65535)>]**

no port-channel load-balance [<port-channel-index(1-65535)>]

Parameter Description

- `src-mac` - Distributes the load based on the source MAC address. The bits of the source MAC address in the packet are used to select the port in which the traffic should flow. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.
- `dest-mac` - Distributes the load based on the destination host MAC address. The bits of the destination MAC address in the packet are used to select the port in which the traffic should flow. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel
- `src-dest-mac` - Distributes the load based on the source and destination MAC address. The bits of the source and destination MAC address in the packet are used to select the port in which the traffic should flow.
- `src-ip` - Distributes the load based on the source IP address. The bits of the source IP address in the packet are used to select the port in which the traffic should flow.
- `dest-ip` - Distributes the load based on the destination IP address. The bits of the destination IP address in the packet are used to select the port in which the traffic should flow.
- `src-dest-ip` - Distributes the load based on the source and destination IP address. The bits of the source and destination IP address in the packet are used to select the port in which the traffic should flow.
- `vlan-id` - Distributes the load distribution based on VLAN ID. The VLAN ID in the packet is used to select the port in which the traffic should flow.
- `service-instance` - Distributes the load based on service-instance. The ISID in the packet is used to select the port in which the traffic should flow. Packets with the same service-instance use the same port. Packets with different service-instance use different ports such that the load is balanced among ports. The port can have packets with different service-instances also.
- `mac-src-vid` - Distributes the load based on source MAC address and VLAN ID. The VLAN ID and

source MAC address in the packet are used to select the port in which the traffic should flow.

- `mac-dest-vid` - Distributes the load based on destination MAC address and VLAN ID. The VLAN ID and destination MAC address in the packet are used to select the port in which the traffic should flow.
- `mac-src-dest-vid` - Distributes the load based on VLAN ID, and destination and source MAC address. The VLAN ID, source MAC address and destination MAC address in the packet are used to select the port in which the traffic should flow.
- `dest-ip6` - Distributes the load based on the destination IP6 address. The bits of the destination IP6 address in the packet are used to select the port in which the traffic should flow.
- `src-ip6` - Distributes the load based on the source IP6 address. The bits of the source IP6 address in the packet are used to select the port in which the traffic should flow.
- `l3-protocol` - Distributes the load based on the Layer 3 protocol. The bits of the Layer 3 protocol in the packet are used to select the port in which the traffic should flow.
- `dest-l4-port` - Distributes the load based on the destination Layer 4 port. The bits of the destination Layer 4 port in the packet are used to select the port in which the traffic should flow.
- `src-l4-port` - Distributes the load based on the source Layer 4 port. The bits of the source Layer 4 port in the packet are used to select the port in which the traffic should flow.
- `mpls-vc-label` - Distributes the load based on MPLS VC label. The MPLS VC label in the packet is used to select the port in which the traffic should flow.
- `mpls-tunnel-label` - Distributes the load based on MPLS tunnel label. The MPLS tunnel label in the packet is used to select the port in which the traffic should flow.
- `mpls-vc-tunnel-label` - Distributes the load based on MPLS VC and tunnel labels. The MPLS VC and tunnel labels in the packet are used to select the port in which the traffic should flow.
- `<port-channel-index(1-65535)>` - Configures the load balancing policy for the specified port-channel. This is a unique value that represents the specific port-channel created. This value ranges between 1 and 65535.

Mode Global Configuration Mode

Default src-dest-mac

Notes:

- This command executes successfully, only if the LA functionality is started and enabled in the switch.
- The following parameters are not supported in BCM target.
  - vlan-id
  - service-instance
  - mac-src-vid
  - mac-dest-vid
  - mac-src-dest-vid
  - dest-ip6
  - src-ip6
  - l3-protocol

- dest-l4-port
- src-l4-port
- mpls-vc-label
- mpls-tunnel-label
- mpls-vc-tunnel-label
- Some parameters are not support for certain SMIS switch models.

Example
```
Your Product(config)# port-channel load-balance dest-mac 1
```

Related Command(s)

- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.
- `set port-channel` - Configures the admin status of LA in the switch.
- `show etherchannel` - Displays Etherchannel information for all port- channel groups created in the switch.
- `interface-configuration and deletion` - Allows to configure interface such as out of band management, port channel, tunnel and so on

lacp port-priority

Command Objective This command configures the LACP port priority. This value ranges between 0 and 65535.

This port priority is used in combination with LACP port identifier during the identification of best ports in a port channel. The priority determines if the link is an active link or a standby link, when the number of ports in the aggregation exceeds the maximum number supported by the hardware. The links with lower priority becomes active links.

The no form of the command resets the LACP port priority to its default value.

Syntax **lacp port-priority <0-65535>**

no lacp port-priority

Mode Interface Configuration Mode (Physical Interface Mode)

Default 128

Notes:

- This command executes successfully, only if the LA functionality is started and enabled in the switch.
- This configuration takes effect only on the interface that is configured for LACP.

Example
```
Your Product(config-if)# lacp port-priority 1
```

Related Command(s)

- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.
- `set port-channel` - Configures the admin status of LA in the switch.
- `channel-group` - Adds the port as a member of the specified port channel that is already created in the switch.
- `default port` - Configures the default port for a port channel.
- `show etherchannel` - Displays Etherchannel information for all port- channel groups created in the switch.
- `show interfaces` - etherchannel - Displays Etherchannel details for all aggregated ports and port channels.
- `show lacp` - Displays LACP counter information for all port-channels.

lacp port-identifier

Command Objective This command configures the LACP actor admin port ID to be filled in the LACP PDUs. This value represents the concerned aggregation port. This value ranges from 1 to 65535.

The maximum limit depends on the board. For example, if the board has only 24 ports, then the maximum value will be 24 only. That is the value ranges from 1 to 24.

Syntax **lacp port-identifier <1-65535>**

Mode Interface Configuration Mode (Physical Interface Mode)

Default The port ID is set as the LACP actor admin port ID.

Notes:

- This command executes successfully, only if the LA functionality is started and enabled in the switch.
- This configuration takes effect only on the interface that is configured for LACP.

Example

```
Your Product(config-if)# lacp port-identifier 2
```

Related Command(s)

- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.
- `set port-channel` - Configures the admin status of LA in the switch.
- `channel-group` - Adds the port as a member of the specified port channel that is already created in the switch.
- `default port` - Configures the port that should be set as default port for a port channel.
- `show etherchannel` - Displays Etherchannel information for all port- channel groups created in the switch.
- `show interfaces` - etherchannel - Displays Etherchannel details for all aggregated ports and port channels.

channel-group

Command Objective This command adds the port as a member of the specified port channel that is already created in the switch.

The no form of the command deletes the aggregation of the port from all port channels.

Syntax **channel-group <channel-group-number(1-65535)> Mode {auto [non-silent] | desirable [non-silent] | on | active | passive }**

no channel-group

Parameter Description

- `<channel-group-number(1-65535)>` - Adds the port as a member of the specified port channel. This is a unique value that represents the specific port-channel created. This value ranges from 1 to 65535.
- `Mode` - Configures the LACP activity for the port:
  - `auto` - Places a port into a passive negotiating state in which the port responds to received PAgP packets, but does not initiate PAgP packet negotiation. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
  - `desirable` - Places a port into an active negotiating state in which the port initiates negotiations with other ports by sending PAgP packets. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
  - `[non-silent]` - Used with the auto or desirable keyword when traffic is expected from the other device. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
  - `active` - Starts LACP negotiation un-conditionally.
  - `passive` - Starts LACP negotiation only when LACP packet is received from peer.
  - `on` - Forces the interface to channel without LACP. This is equivalent to manual aggregation.

Mode Interface Configuration Mode (Physical Interface Mode)

Note: This command can be executed successfully, only if the LA functionality is started and enabled in the switch.

Example Your Product(config-if)# channel-group 1 Mode active

Related Command(s)

- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.
- `set port-channel` - Configures the admin status of LA in the switch.
- `lacp port-priority` - Configures the LACP port priority.
- `lacp port-identifier` - Configures the LACP actor admin port ID to be filled in the LACP PDUs.
- `lacp wait-time` - Configures the LACP wait-time for an interface.

- `lacp timeout` - Configures the LACP timeout period within which LACPDUs should be received on a port to avoid timing out of the aggregated link.
- `default port` - Configures the port that should be set as default port for a port channel.
- `show etherchannel` - Displays Etherchannel information for all port- channel groups created in the switch.
- `show interfaces` - etherchannel - Displays Etherchannel details for all aggregated ports and port channels.
- `show lacp` - Displays LACP counter / neighbor information for all port- channels.
- `interface-configuration and deletion` - Allows to configure interface such as out of band management, port channel, tunnel and so on.

lacp wait-time

Command Objective This command configures the LACP wait-time for an interface. This value ranges from 0 to 10 seconds.

The wait time represent the time (in seconds) till which the port waits before entering into aggregation after receiving partner information (that is, this represents the time taken to attach to the port channel).

The no form of the command resets the LACP wait-time to its default value.

Syntax **lacp wait-time <0-10>**

no lacp wait-time

Mode Interface Configuration Mode (Physical Interface Mode)

Default 2

Notes:

- This command can be executed successfully, only if the LA functionality is started and enabled in the switch.
- This configuration takes effect only on the interface that is configured for LACP.

Example

```
Your Product(config-if)# lacp wait-time 1
```

Related Command(s)

- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.
- `set port-channel` - Configures the admin status of LA in the switch.
- channel-group - Adds the port as a member of the specified port channel that is already created in the switch.
- `default port` - Configures the port that should be set as default port for a port channel.
- `show etherchannel` - Displays Etherchannel information for all port- channel groups created in the switch.

- show interfaces - etherchannel - Displays Etherchannel details for all aggregated ports and port channels.

lacp timeout

Command Objective This command configures the LACP timeout period within which LACPDUs should be received on a port to avoid timing out of the aggregated link.

The no form of the command sets the LACP timeout period to its default value.

Syntax **lacp timeout {long | short }**

no lacp timeout

Parameter Description

- long - Configures the LACP timeout period as 90 seconds. The LACP PDU is sent every 30 seconds.
- short - Configures the LACP timeout period as 3 seconds. The LACP PDU is sent every second.

Mode Interface Configuration Mode (Physical Interface Mode)

Default long

Notes:

- This command can be executed successfully, only if the LA functionality is started and enabled in the switch.
- This configuration takes effect only on the interface that is configured for LACP.

Example

```
Your Product(config-if)# lacp timeout short
```

Related Command(s)

- shutdown port-channel - Shuts down LA in the switch and releases the allocated resources to the switch.
- set port-channel - Configures the admin status of LA in the switch.
- channel-group - Adds the port as a member of the specified port channel that is already created in the switch.
- default port - Configures the port that should be set as default port for a port channel.
- show etherchannel - Displays Etherchannel information for all port- channel groups created in the switch.
- show interfaces - etherchannel - Displays Etherchannel details for all aggregated ports and port channels.
- show lacp - Displays LACP counter / neighbor information for all port- channels.

lacp rate

Command Objective This command configures the LACP rate. This command is a standardized implementation of the existing command; `lacp timeout`. It operates similar to the existing command.

The no form of the command sets the LACP rate to its default value.

Syntax **lacp rate {normal | fast }**

no lacp rate

Parameter Description

- normal - Ingresses the LACP control packets at normal rate. That is, LACP PDU is sent every 30 seconds and the timeout value (no packet is received from peer) is set as 90 seconds.
- fast - Ingresses the LACP control packets at fast rate. That is, LACP PDU is sent every 1 second and the timeout value is set as 3 seconds.

Mode Interface Configuration Mode (Physical Interface Mode)

Default normal

Notes:

- This command can be executed successfully, only if the LA functionality is started and enabled in the switch.
- This configuration takes effect only on the interface that is configured for LACP.

Example Your Product(config-if)# lacp rate fast

Related Command(s)

- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.
- `set port-channel` - Configures the admin status of LA in the switch.
- `channel-group` - Adds the port as a member of the specified port channel that is already created in the switch.
- `lacp timeout` - Configures the LACP timeout period.
- `default port` - Configures the port that should be set as default port for a port channel.
- `show etherchannel` - Displays Etherchannel information for all port- channel groups created in the switch.
- `show interfaces` - etherchannel - Displays Etherchannel details for all aggregated ports and port channels.
- `show lacp` - Displays LACP counter / neighbor information for all port- channels.

lacp admin-key

Command Objective This command configures the LACP actor admin key and LACP Mode for a port.

Syntax **lacp admin-key <(Admin Key)1-65535> [Mode {active | passive}]**

Parameter Description

- `admin-key` - Configures the LACP actor admin key that is used while port participates in dynamic aggregation selection. The port is made as part of best aggregation selected based on system ID and admin key.This value ranges between 1 and 65535.
- `Mode` - Configures the LACP Mode for the port. The different options are:
  - `active` - Starts LACP negotiation un-conditionally.
  - `passive` - Starts LACP negotiation only when LACP packet is received from peer.

Mode Interface Configuration Mode (Physical Interface Mode)

Default Mode - active

Notes:

- This command can be executed successfully, only if the LA functionality is started and enabled in the switch.
- The admin key can be configured only for ports that select aggregator dynamically (the port is configured as default interface for a port channel)

Example

```
Your Product(config-if)# lacp admin-key 1 Mode active
```

Related Command(s)

- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.
- `set port-channel` - Configures the admin status of LA in the switch.
- `default port` - Configures the default port for a port channel.
- `show etherchannel` - Displays Etherchannel information for all port- channel groups created in the switch.
- `show interfaces` - etherchannel - Displays Etherchannel details for all aggregated ports and port channels.
- `show lacp` - Displays LACP counter / neighbor information for all port- channels.

default port

Command Objective This command configures the port that should be set as default port for a port channel. The configured port attaches with the port channel and participates only in dynamic aggregation selection.

The no form of the command deletes the default port assigned for the port channel.

Syntax **default port <interface-type> <interface-id>**

no default port

Parameter Description

- `<interface-type>` - Configures the type of interface to be set as default port for the port channel. The interface can be:
  - `fastethernet` – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `i-lan`– Internal LAN created on a bridge per IEEE 802.1ap.
- `<interface-id>`- Configures the ID of the interface to be set as default port. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan ID is provided, for interface type i-lan. For example: 1 represents i-lan ID.

Mode Interface Configuration Mode (Port Channel Interface Mode)

Notes:

- This command can be executed successfully, only if the LA functionality is started and enabled in the switch.
- Only one port can be set as a default port.
- The port that is to be set as default port should have not been added as a member port for any of the port channel.

Example

```
Your Product(config-if)# default port gigabitethernet 0/1
```

Related Command(s)

- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.
- `set port-channel` - Configures the admin status of LA in the switch.
- `lacp port-priority` - Configures the LACP port priority.
- `lacp port-identifier` - Configures the LACP actor admin port ID to be filled in the LACP PDUs.
- `no channel-group` - Deletes the aggregation of the port from all port channels.
- `lacp wait-time` - Configures the LACP wait-time for an interface.
- `lacp timeout` - Configures the LACP timeout period within which LACPDUs should be received on a port to avoid timing out of the aggregated link.
- `lacp admin-key` - Configures the LACP actor admin key and LACP Mode for a port.
- `show etherchannel` - Displays Etherchannel information for all port- channel groups created in the switch.
- `show interfaces` - etherchannel - Displays Etherchannel details for all aggregated ports and port

channels.

- `show lacp` - Displays LACP counter / neighbor information for all port- channels.

port-channel max-ports

Command Objective This command configures the maximum number of ports that can be attached to a port channel. This value ranges between 2 and 8.

The best ports are maintained in active state and other ports are maintained in standby state, if the total number of ports attached to the port-channel exceeds the configured value.

Syntax **port-channel max-ports <integer (2-8)>**

Mode Interface Configuration Mode (Port Channel Interface Mode)

Default 8

Note: This command can be executed successfully, only if the LA functionality is started and enabled in the switch.

Example

```
Your Product(config-if)# port-channel max-ports 5
```

Related Command(s)

- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.
- `set port-channel` - Configures the admin status of LA in the switch.

debug lacp

Command Objective This command enables the tracing of the LACP as per the configured debug levels. The trace statements are generated for the configured trace levels. This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

The no form of the command disables the tracing of the LACP as per the configured debug levels. The trace statements are not generated for the configured trace levels

Syntax **debug lacp [{ init-shutdown | mgmt | data | events | packet | os | failall | buffer | all }]**
no debug lacp [{ init-shutdown | mgmt | data | events | packet | os | failall | buffer | all }]

Parameter Description

- `init-shutdown` - Generates debug statements for init and shutdown traces. These traces are generated during module initialization and shutdown.
- `mgmt` - Generates debug statements for management traces. This trace is generated whenever you

configure any of the LA features.

- `data` - Generates debug statements for data path traces. This trace is generated during failure in packet processing.
- `events` - Generates debug statements for event traces. This trace is generated when any of packets are sent successfully or when an ACK is received.
- `packet` - Generates debug statements for packet dump traces. This trace is generated for all events generated during processing of packets.
- `os` - Generates debug statements for OS resource related traces. This trace is generated during failure in message queues.
- `failall` - Generates debug statements for all kind of failure traces.
- `buffer` - Generates debug statements for buffer related traces.
- `all` - Generates debug statements for all kinds of traces.

Mode Privileged EXEC Mode

Default init-shutdown

Example

```
Your Product# debug lacp data
```

debug etherchannel

Command Objective This command enables the tracing of the link aggregation module as per the configured debug levels. The trace statements are generated for the configured trace levels. This command is a standardized implementation of the existing command; `debug lacp`. It operates similar to the existing command.

The no form of the command disables the tracing of the link aggregation as per the configured debug levels. The trace statements are not generated for the configured trace levels

Syntax **debug etherchannel {[all] [detail] [error] [event] [idb]}**

no debug etherchannel {[all] [detail] [error] [event] [idb]}

Parameter Description

- `all` - Generates debug statements for all kinds of traces.
- `detail` - Generates detailed debug statements for traces.
- `error` - Generates debug statements for all failure traces.
- `event` - Generates debug statements for event traces. This trace is generated when any of packets are sent successfully or when an ACK is received. Event generates error messages for the following scenarios
    - Packet reception/transmission
    - Timer expiry
    - Port creation/deletion indication
    - Port status change indication

- `idb` - Generates debug statements for interface descriptor block traces. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Privileged EXEC Mode

Example `Your Product# debug etherchannel detail`

show etherchannel

Command Objective This command displays Etherchannel information for all port-channel groups created in the switch. This information contains admin and oper status of port- channel module, and status of protocol operate Mode for each group.

Syntax **show etherchannel [[channel-group-number] { detail | load- balance | port | port-channel | summary | protocol | redundancy}]**

Parameter Description

- `channel-group-number` - Displays Etherchannel information for the specified port-channel group. This is a unique value that represents the specific port-channel created. This value ranges from 1 to 65535.
- `detail` - Displays detailed Etherchannel information. The information contain admin and oper status of port channel module, LACP system priority, status of protocol operate Mode for each group, port details for each group and port channel details. The port details contain port state, group to which the port belongs, port Mode, aggregation state, port-channel ID, pseudo port- channel ID, admin key, oper key, port number, port state, and LACP port-priority, wait-time, port identifier, activity and timeout. The port channel details contain port channel ID, number of member ports, ID of hot standby port, port state, status of protocol operate Mode, aggregator MAC and default port ID.
- `load-balance` - Displays the load balancing policy applied for each port- channel groups.
- `port` - Displays the status of protocol operate Mode and port details for each group. The port details contain port state, group to which the port belongs, port Mode, aggregation state, port- channel ID, pseudo port- channel ID, admin key, oper key, port number, port state, and LACP port- priority, wait-time, port identifier, activity and timeout.
- `port-channel` - Displays the admin and oper status of port channel module, and port channel details. The port channel details contain port channel ID, number of member ports, ID of hot standby port, port state, status of protocol operate Mode, aggregator MAC and default port ID.
- `summary` - Displays the admin and oper status of port channel module, number of channel groups used, number of aggregators, group IDs, and port channel ID, status of protocol operate Mode and member ports for each group.
- `protocol` - Displays the status of protocol operate Mode for each port- channel group.
- `redundancy` - Displays the actor information and synchronized partner information for the port, port state flags decode information, and aggregation state. The actor information contain channel group ID, pseudo port channel ID and currentwhile split interval timer count value. The partner information contains partner system ID, flags, LACP partner port priority and LACP partner oper key.

The decode information contain LACP activity and LACP timeout.

Mode Privileged EXEC Mode

Note: This command executes successfully, only if the LA functionality is started and enabled in the switch.

Example `Your Product# show etherchannel`

```
Port-channel Module Admin Status is enabled

Port-channel Module Oper Status is enabled
Port-channel System Identifier is 00:01:02:03:04:01
                        Channel Group Listin
                        ---------------------------------
Group : 1
----------------
Protocol : LACP
Your Product# show etherchannel 1 detail Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel System Identifier is 00:01:02:03:04:01
LACP System Priority: 32768
                        Channel Group Listing
                        ---------------------------------
Group: 1
----------------
Protocol :LACP
                        Port : Gi0/1
                        --------------------
Ports in the Group
----------------------------
Port State = Up in Bundle
Channel Group : 1
Mode : Active
Pseudo port-channel = Po1
LACP port-priority = 128
LACP Wait-time = 2 secs
LACP Activity : Active
LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting, Distributing, Defaulted
                        LACP Port       Admin        Oper   Port   Port
Port                    State           Priority     Key    Key    Number       State
----------------------------------------------------------------------------
Gi0/1                   Bundle          128          1      1      0x1          0xbe
Port-channel : Po1
----------------------------
Number of Ports = 1
HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = LACP
Aggregator-MAC 00:01:02:03:04:19
Default Port = None
Your Product# show etherchannel 1 port
                        Channel Group Listing
                        ---------------------------------
Group: 1
```

```
----------------
Protocol :LACP
                                        Ports in the Group
                                        ------------------
Port : Gi0/1
------------
Port State = Up in Bundle
Channel Group : 1
Mode : Active
port-channel = Po1
Pseudo port-channel = Po1
LACP port-priority = 128
LACP Wait-time = 2 secs
LACP Port Identifier = 2
LACP Activity : Active
LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting, Distributing,
Port : Gi0/2
------------
Port State = Up in Bundle
Channel Group : 1
Mode : Active
port-channel = Po1
                        Pseudo port-channel = Po1
LACP port-priority = 128
LACP Wait-time = 2 secs
LACP Activity : Active
LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting, Distributing,
                                 LACP Port     Admin  Oper   Port          Port
Port                    State    Priority      Key    Key    Number        State
------------------------------------------------
Gi0/1                   Bundle   128           1      1      0x1           0xbc
Gi0/2                   Bundle   128           1      1      0x2           0xbc
Your Product# show etherchannel 1 port-channel
Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel System Identifier is 00:01:02:03:04:01
                        Channel Group Listing
                        ---------------------
Group : 1
----------
                        Port-channels in the group:
                        ---------------------------
Port-channel : Po1
-------------------
Number of Ports = 1
HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = LACP
Aggregator-MAC 00:01:02:03:04:19
Default Port = None
Your Product# show etherchannel 1 summary
Flags:
D - down        P - in port-channel
I - stand-alone S - suspended
```

```
H - Hot-standby (LACP only)
Port-channel is enabled
Port-channel System Identifier is 00:01:02:03:04:05
Number of channel-groups in use: 1
Number of aggregators: 1
Group                   Port-channel    Protocol     Ports
----------------------------------------------------------
1                       Po1(P)          LACP         Gi0/1(P),Gi0/2(P)
Your Product# show etherchannel 1 protocol
                        Channel Group Listing
                        ---------------------
Group : 1
----------
Protocol : LACP
Your Product# show etherchannel load-balance
                        Channel Group Listing
                        ---------------------
Group : 1
----------
Source & Destination MAC Address
Your Product# show etherchannel redundancy
Actor Information for Port : Gi0/1
----------------------------------
Channel Group : 1
Pseudo port-channel = Po1
CurrentWhile Split Interval Tmr Count = 1
Synced Partner Information for Port : Gi0/1
-----------------------------------
Partner System ID                 : 00:11:22:33:44:55
Flags                             : A
LACP Partner Port Priority        : 128
LACP Partner Oper Key             : 1
Port State Flags Decode
------------------------
Activity : Active
LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting, Distributing,
Actor Information for Port : Gi0/2
-------------
Channel Group : 1
Pseudo port-channel = Po1
CurrentWhile Split Interval Tmr Count = 1
Synced Partner Information for Port : Gi0/2
-------------
Partner System ID                 : 00:11:22:33:44:55
Flags                             : A
LACP Partner Port Priority        : 128
LACP Partner Oper Key             : 1
Port State Flags Decode
------------------------
Activity : Active
LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting, Distributing,
```

Related Command(s)

- shutdown port-channel - Shuts down LA in the switch and releases the allocated resources to the switch.
- set port-channel - Configures the admin status of LA in the switch.
- lacp system-priority - Configures the LACP priority that is associated with actor's system ID.
- port-channel load-balance - Configures the load balancing policy for all port channels created in the switch.
- lacp port-priority - Configures the LACP port priority.
- lacp port-identifier - Configures the LACP actor admin port ID to be filled in the LACP PDUs.
- channel-group - Adds the port as a member of the specified port channel that is already created in the switch.
- lacp wait-time - Configures the LACP wait-time for an interface.
- lacp timeout - Configures the LACP timeout period within which LACPDUs should be received on a port to avoid timing out of the aggregated link.
- lacp admin-key - Configures the LACP actor admin key and LACP Mode for a port.
- default port - Configures the port that should be set as default port for a port channel.
- interface-configuration and deletion - Allows to configure interface such as out of band management, port channel, tunnel and so on.

show interfaces - etherchannel

Command Objective This command displays Etherchannel details for all aggregated ports and port channels. The port details contain port state, group to which the port belongs, port Mode, aggregation state, port-channel ID, pseudo port-channel ID, admin key, oper key, port number, port state, and LACP port-priority, wait-time, port identifier, activity and timeout.

The port channel details contain port channel ID, number of member ports, ID of hot standby port, port state, status of protocol operate Mode, aggregator MAC and default port ID.

Syntax **show interfaces [<interface-type> <interface-id>]**

etherchannel

Parameter Description

- <interface-type> - Displays the Etherchannel details for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- <interface-id> - Displays the Etherchannel details for the specified interface identifier. This is a

unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that theslot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For example: 1 represents port-channel ID.

Mode Privileged EXEC Mode

Note: This command executes successfully, only if the LA functionality is started and enabled in the switch.

Example `Your Product# show interfaces gigabitethernet 0/1 etherchannel`

```
Port : Gi0/1
--------------------
Port State = Up in Bundle
Channel Group : 2
Mode : Active
Pseudo port-channel = Po2
LACP port-priority = 128
LACP Port Identifier = 2
LACP Wait-time = 2 secs
LACP Activity : Passive
LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting, Distributing,
                                  LACP Port     Admin  Oper   Port          Port
Port                     State    Priority      Key    Key    Number        State
----------------------------------------------------------------------------------------------
Gi0/1                    Bundle   128           2      2      0x1           0x3c
Your Product# show interfaces etherchannel
Port : Gi0/1
--------------------
Port State = Up in Bundle
Channel Group : 2
Mode : Active
Pseudo port-channel = Po2
LACP port-priority = 128
LACP Wait-time = 2 secs LACP Activity : Passive LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting, Distributing,
Port : Gi0/2
--------------------
Port State = Up in Bundle
Channel Group : 2
Mode : Active
Pseudo port-channel = Po2
LACP port-priority = 128
LACP Wait-time = 2 secs LACP Activity : Passive LACP Timeout : Long
SMIS
Aggregation State : Aggregation, Sync, Collecting, Distributing,
                                  LACP Port     Admin  Oper   Port          Port
Port                     State    Priority      Key    Key    Number        State
------------------------------------------------------------------------------------------------------------
Gi0/1                    Bundle   128           2      2      0x1           0x3c
```

```
Gi0/2                   Bundle   128          2      2      0x2           0x3c
Port-channel : Po2
------------------- Number of Ports = 2
HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = LACP
Aggregator-MAC 00:01:02:03:04:23
Default Port = None
```

Related Command(s)

- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.
- `set port-channel` - Configures the admin status of LA in the switch.
- `lacp port-priority` - Configures the LACP port priority.
- `lacp port-identifier` - Configures the LACP actor admin port ID to be filled in the LACP PDUs.
- `channel-group` - Adds the port as a member of the specified port channel that is already created in the switch.
- `lacp wait-time` - Configures the LACP wait-time for an interface.
- `lacp timeout` - Configures the LACP timeout period within which LACPDUs should be received on a port to avoid timing out of the aggregated link.
- `lacp admin-key` - Configures the LACP actor admin key and LACP Mode for a port.
- `default port` - Configures the port that should be set as default port for a port channel.

show lacp

Command Objective This command displays LACP counter / neighbor information for all port- channels.

Syntax show lacp [<port-channel(1-65535)>] { counters | neighbor [detail] }

Parameter Description

- `<port-channel(1-65535)>` - Displays LACP counter / neighbor information for the specified port-channel. This is a unique value that represents the specific port-channel created. This value ranges from 1 to 65535.
- `counters` - Displays the LACP counter information. The information contains port ID, LACPDUs sent and received, number of markers sent and received, number of marker response sent and received, number of LACPDUs packets and number of LACPDUs errors.
- `neighbor [detail] - neighbor` - Displays LACP neighbor information. This information contains partner system ID, flags details, LACP partner port priority, operational key, and port state. detail - Displays detailed LACP neighbor information. This information contains partner system ID, flags, aggregation state, and LACP partner port priority, partner oper key, partner port state, activity and timeout.

Mode Privileged EXEC Mode

Note: This command can be executed successfully, only if the LA functionality is started and enabled in the switch.

Example

```
Your Product# show lacp 1 counters

                        LACPDUs         Marker       Marker Response
LACPDUs
Port                    Sent      Recv   Sent   Recv   Sent   Recv   Pkts   Err
------------------------------------------------------------------------------
Channel group: 1
------------------
Gi0/1                   394       352    0      0      0      0      0      0
Gi0/2                   318       297    0      0      0      0      0      0
Your Product# show lacp neighbor detail
Flags:
A - Device is in Active Mode
P - Device is in Passive Mode
Channel group 1 neighbors
Port Gi0/1
----------
Partner System ID               : 00:01:02:03:04:21
Flags                           : P LACP Partner Port Priority     : 128
LACP Partner Oper Key           : 2
LACP Partner Port State         : 0x3c
Port State Flags Decode
------------------------
Activity : Passive
LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting, Distributing
Port Gi0/2
----------
Partner System ID               : 00:01:02:03:04:21
Flags                           : P LACP Partner Port Priority     : 128
LACP Partner Oper Key           : 2
LACP Partner Port State         : 0x3c
Port State Flags Decode
------------------------
Activity : Passive
LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting, Distributing
```

Related Command(s)

- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.
- `set port-channel` - Configures the admin status of LA in the switch.
- `lacp port-priority` - Configures the LACP port priority.
- `channel-group` - Adds the port as a member of the specified port channel that is already created in the switch.
- `lacp timeout` - Configures the LACP timeout period within which LACPDUs should be received on a port to avoid timing out of the aggregated link.
- `lacp admin-key` - Configures the LACP actor admin key and LACP Mode for a port.
- `default port` - Configures the port that should be set as default port for a port channel.

- interface-configuration and deletion - Allows to configure interface such as out of band management, port channel, tunnel and so on.

mlag portal-address

Command Objective This command configures the MAC address component of MLAG portal system ID. The system ID denotes a 6-octet unicast MAC address value that is used as a unique identifier for the switch containing the MLAG enabled port-channel.

The no form of this command removes the association.

Syntax **mlag portal-address <xx:xx:xx:xx:xx:xx>**

no mlag

Parameter Description <xx:xx:xx:xx:xx:xx> – Specifying the MAC address of portal system ID

Mode Interface Configuration Mode

Example

```
SMIS(config)# interface po 1
SMIS(config-if)# mlag portal-address 00:30:48:00:00:01
SMIS(config-if)# exit
SMIS(config)#
```

Related Command(s)

- mlag portal-priority – Configure the priority part of portal system ID for a specified MLAG instance.
- mlag portal-system-number – Configure the portal system number for a specified MLAG instance.
- mlag IPP – Configure IPP link for a specified MLAG instance.

mlag portal-priority

Command Objective This command configures the priority component of MLAG portal system ID. This value ranges between 0 and 65535.

No form of this command removes the association.

Syntax **mlag portal-priority <0-65535>**

no mlag

Parameter Description <0-65535> – Specifying the priority of portal system ID

Mode Interface Configuration Mode

Example

```
SMIS(config)# interface po 1
SMIS(config-if)# mlag portal-priority 32767
SMIS(config-if)# exit
SMIS(config)#
```

Related Command(s)

- `mlag portal-address` – Configure the MAC address part of portal system ID for a specified MLAG instance.
- `mlag portal-system-number` – Configure the portal system number for a specified MLAG instance.
- `mlag IPP` – Configure IPP link for a specified MLAG instance.

mlag portal-system-number

Command Objective This command configures the system number for a specified MLAG instance.

No form of this command removes the association.

Syntax **mlag portal-system-number <1-3>**

no mlag

Parameter Description `<1-3>` – Specifying the portal system number

Mode Interface Configuration Mode

Note: The portal-system-number is a unique identifier for the switch in an MLAG domain. Each switch can has multiple MLAG-enabled port-channels but the portal-system-number of each configured MLAG-enabled port-channel must be the same.

Example

```
SMIS(config)# interface po 1
SMIS(config-if)# mlag portal-system-number 1
SMIS(config-if)# exit
SMIS(config)#
```

Related Command(s)

- `mlag portal-priority` - Configure the priority part of portal system ID for a specified MLAG instance.
- `mlag portal-system-number` – Configure the portal system number for a specified MLAG instance.
- `mlag IPP` – Configure IPP link for a specified MLAG instance.

show mlag

Command Objective This command displays MLAG counter / portal information for all MLAG port-channel.

Syntax **show mlag [<port-channel(1-65535)>] { counters | detail }**

Parameter Description

- `<port-channel(1-65535)>` - Displays MLAG counter / portal information for the specified MLAG port-channel. This is a unique value that represents the specific port-channel created. This value ranges from 1 to 65535.
- `counters` - Displays the MLAG counter information. The information contains port ID, DRCPDUs and ASPDUs sent and received, number of LACPDUs errors.
- `detail` - Displays MLAG portal information. This information contains portal state, configuration check result, portal role, portal system ID, portal system number, assigned IPP port, aggregator ID, active member ports and MLAG neighbor information.

Mode Privileged EXEC Mode

The portal-system-number is a unique identifier for the switch in an MLAG domain. Each switch can has multiple MLAG-enabled port-channels but the portal-system-number of each configured MLAG-enabled port-channel must be the same.

Example

```
Your Product# show mlag detail
show mlag detail
MLAG Configuration : Channel Group 200
----------------------------------------------------------------------------------------
Portal State : Normal State
Configuration Check Result : No inconsistency found
Portal Role : SECONDARY

Portal System Address : 00:11:22:33:44:55
Portal System Priority : 128
Portal System Number : 1
Intra-Portal-Port : port-channel 100
Three Portal System : 0
Aggregator Address : 0c:c4:7a:1a:43:a8
Aggregator Priority : 32768
Active ports ifIndex : 60
Neighbor Portal System Address : 00:11:22:33:44:55
Neighbor Portal System Priority : 128
Neighbor Portal System Number : 2
Neighbor Portal Three Portal System : 0
Neighbor Portal Aggregator Address : 0c:c4:7a:1a:44:3e
Neighbor Portal Aggregator Priority : 32768
Neighbor Portal Partner Aggregator Key : 200
Active ports ifIndex : 60

Your Product# show mlag counters
```

```
MLAG Global Statistics:
------------------------------------------------------------
DRCPDU Overflow         : 0
ASPDU Sent              : 55
ASPDU Recv              : 267
ASPDU Err               : 1
ASPDU Overflow          : 0
FDBSYNC Send            : 54
FDBREQ  Send            : 13
FDBSYNC Recv            : 39
FDBREQ  Recv            : 230
Pending FDBREQ          : 0
MLAG IPP Statistics for Channel group: 200
---------------------------------------------------
IPP             : port-channel 100
DRCPDU Sent                : 147
DRCPDU Recv                : 78
DRCPDU Err                 : 0
MLAG IPP Statistics for Channel group: 500
----------------------------------------------------------------------------------
IPP                        : port-channel 100
DRCPDU Sent                : 81
DRCPDU Recv                : 56
DRCPDU Err                 : 0
```

Related Command(s)

- `mlag portal-priority` - Configure the priority part of portal system ID for a specified MLAG instance.
- `mlag portal-address` – Configure the MAC address part of portal system ID for a specified MLAG instance.
- `mlag portal-system-number` – Configure the portal system number for a specified MLAG instance.
- `mlag IPP` – Configure IPP link for a specified MLAG instance.

19 LLDP

LLDP (Link Layer Discovery Protocol) supports a set of attributes that it uses to discover the neighbor devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP supported devices can use TLVs to receive and send information to their neighbors.

The switch supports these mandatory basic management TLVs.

- Port description TLV
- System name TLV
- System description
- System capabilities TLV
- Management address TLV

- Port VLAN ID TLV ((IEEE 802.1 organizationally specific TLVs)
- MAC/PHY configuration/status TLV(IEEE 802.3 organizationally specific TLVs)

SMIS LLDP is a software implementation of the Link Layer Discovery Protocol (LLDP). It provides complete management capabilities using SNMP and CLI.

SMIS LLDP conforms to IEEE 802.1AB-2005 standard. The LLDP allows systems on an Ethernet LAN to advertise their key capabilities and also to learn about the key capabilities of other systems on the same Ethernet LAN. This, in turn, promotes a unified network management view of the LAN topology and connectivity to aid network administration and trouble-shooting.

SMIS LLDP provides the following features:

- Provides full conformance to the 802.1AB specification.
- Supports all mandatory TLVs (Chassis ID, Port ID and Time To Live).
- Supports optional TLVs - Port description, System name, System description, System capabilities and Management address.
- Supports organizationally specific optional TLVs - Port VLAN ID, Port and protocol VLAN ID, VLAN name, MAC or PHY configuration or status, Link Aggregation and Maximum frame size.
- Provides a generic set of APIs for easy integration into different platforms.
- Supports the basic MIB, as well as, the extension MIBs in Appendix F and Appendix G, defined in the 802.1AB specification and a proprietary MIB for management.
- Provides support for configuration and management by providing generic APIs usable from different management schemes like SNMP, CLI.
- Provides support for notifications through Traps.
- Conforms to Flexible Software Architecture for Portability (FSAP2), thus ensuring portable code, which uses flexible buffer and timer management libraries.

The list of CLI commands for the configuration of LLDP is as follows:

- shutdown lldp
- set lldp
- lldp transmit-interval
- lldp holdtime-multiplier
- lldp reinitialization-delay
- lldp tx-delay
- lldp notification-interval
- lldp chassis-id-subtype
- clear lldp counters
- clear lldp table
- lldp transmit / receive
- lldp notification
- lldp tlv-select basic-tlv
- lldp port-id-subtype
- lldp tlv-select dot1tlv
- lldp tlv-select dot3tlv

- debug lldp
- show lldp
- show lldp interface
- show lldp neighbors
- show lldp traffic
- show lldp local
- show lldp errors
- show lldp statistics
- lldp dest-mac
- set lldp version
- lldp txCreditMax
- lldp MessageFastTx
- lldp txFastInit
- show lldp peer

shutdown lldp

Command Objective This command shuts down all the ports in the LLDP and releases all the allocated memory.

The no form of the command enables all the ports by allocating the required resources in the LLDP

Syntax **shutdown lldp**

no shutdown lldp

Mode Global Configuration Mode

Package Workgroup, Enterprise, Metro and Metro_E

Note: LLDP cannot be started in the switch, if the base bridge Mode is configured as transparent bridging.

Example Your Product(config)# shutdown lldp

Related Command(s)

- `base bridge-Mode` - Configures the base Mode (either 802.1d transparent bridge Mode or 802.1q vlan aware bridge Mode) in which the VLAN feature should operate on the switch.
- `set lldp`- Transmits or receives LLDP frames from the server to the LLDP module
- `lldp transmit / receive` - Transmits or receives LLDP frames from the one of the ports of the server to the LLDP module.
- `lldp tlv-select basic-tlv` - Enables the basic settings while transmitting the LLDP frames on a given port.
- `lldp tlv-select dot1tlv` – Configures dot1 TLV while transmitting the LLDP frames to the particular port

- `lldp tlv-select dot3tlv` - Configures dot3 TLV while transmitting the LLDP frames to the particular port
- `lldp transmit-interval` - Sets the transmission time interval in which the server sends the LLDP frames to the LLDP module.
- `lldp holdtime-multiplier` - Sets the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP
- `lldp reinitialization-delay` - Sets the reinitialization delay time which is the minimum time an LLDP port will wait before reinitializing LLDP transmission.
- `lldp tx-delay` - Sets the transmit delay which is the minimum amount of delay between successive LLDP PDUs.
- `lldp notification` - Controls the transmission of LLDP notifications.
- `lldp notification-interval` - Sets the notification interval which is the minimum interval to generate a notification-event about a change in local system.
- `lldp chassis-id-subtype` - Configures an ID for LLDP chassis subtype which is a unique address of any module.
- `lldp port-id-subtype` - Configures an ID for LLDP port subtype
- `clear lldp counters` - Clears the inbuilt counter which has the total count of LLDP frames transmitted/received.
- `clear lldp table` - Clears all the LLDP information about the neighbors.
- `debug lldp` - Specifies debug level for LLDP module.
- `show lldp` - Displays the LLDP global configuration details to initialize on an interface.
- `show lldp interface` - Displays the information about interfaces where LLDP is enabled.
- `show lldp neighbors` - Displays information about neighbors on an interface or all interfaces.
- `show lldp traffic` - Displays LLDP counters on all interfaces or on a specific interface
- `show lldp local` - Displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.
- `show lldp errors` - Displays the information about the errors such as memory allocation failures, queue overflows and table overflow
- `show lldp statistics` - Displays the LLDP remote table statistics information.
- `lldp dest-mac` - Configures destination mac-address to be used by the LLDP agent for transmission on this port.
- `set lldp version` - Enables the lldp version to be used on the ports.
- `lldp txtCreditMax` - Configures the maximum number of consecutive LLDPDUs that can be transmitted any time
- `lldp MessageFastTx` - Configures the interval at which LLDP frames are transmitted on behalf of this LLDP agent during fast transmission period.
- `lldp txFastInit` - Configures the initial value used to initialize the txFast variable which determines the number of transmissions that are made in fast transmission mode

set lldp

Command Objective This command transmits or receives LLDP frames from the server to the LLDP module.

Syntax **set lldp {enable | disable}**

Parameter Description

- `enable` - Transmits/receives the LLDP packets between LLDP module and the server.
- `disable` - Does not transmit/receive the LLDP packets between LLDP module and the server.

Mode Global Configuration Mode

Default Disable

Note: This command executes only if lldp is started

Example

```
Your Product(config)# set lldp enable
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp` - Displays LLDP global configuration details
- `show lldp interface` - Displays the information about interfaces where LLDP is enabled .
- `show lldp neighbors` - Displays information about the neighbors on an interface or all interfaces.
- `show lldp traffic` - Displays LLDP counters on all interfaces or on a specific interface
- `show lldp errors` - Displays the information about the errors such as memory allocation failures, queue overflows and table overflow.
- `show lldp statistics` - Displays the LLDP remote table statistics information.

lldp transmit-interval

Command Objective This command sets the transmission interval in which the server sends the LLDP frames to the LLDP module. The value ranges between 5 and 32768 seconds.

The no form of the command sets the transmission interval to the default value

Syntax **lldp transmit-interval <seconds(5-32768)>**

no lldp transmit-interval

Mode Global Configuration Mode

Default 30 seconds

Note: This command executes only if lldp is started

Example

```
Your Product(config)# lldp transmit-interval 50
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp` - Displays LLDP global configuration details

lldp holdtime-multiplier

Command Objective This command sets the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP. The value ranges between 2 and 10 seconds.

The no form of the command sets the multiplier to the default value

Note: TLV (Time to Live) A value that tells the receiving agent, how long the information contained in the TLV Value field is valid.

TTL = message transmission interval * hold time multiplier.

For example, if the value of LLDP transmission interval is 30, and the value of the LLDP hold multiplier is 4, then the value 120 is encoded in the TTL field in the LLDP header.

Syntax **lldp holdtime-multiplier <value(2-10)>**

no lldp holdtime-multiplier

Mode Global Configuration Mode

Default 4

Note: This command executes only if lldp is started

Example

```
Your Product(config)# lldp holdtime-multiplier 5
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp` - Displays LLDP global configuration details.
- `lldp tx-delay` - Sets transmit delay which is the minimum amount of delay between successive LLDP frame transmissions.

lldp reinitialization-delay

Command Objective This command sets the reinitialization delay time which is the minimum time an LLDP port will wait before reinitializing LLDP transmission. The value ranges between 1 and 10 seconds.

The no form of the command sets the reinitialization delay time to the default value.

Syntax **lldp reinitialization-delay <seconds(1-10)>**

no lldp reinitialization-delay

Mode Global Configuration Mode

Default 2 seconds

Note: This command executes only if lldp is started

Example

```
Your Product(config)# lldp reinitialization-delay 4
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp` - Displays LLDP global configuration details

lldp tx-delay

Command Objective This command sets the transmit delay which is the minimum amount of delay between successive LLDP frame transmissions. The value ranges between 1 and 8192 seconds.

The no form of the command sets the transmit delay to the default value.

Note: TxDelay should be less than or equal to (0.25 * Message Tx Interval)

Syntax **lldp tx-delay <seconds(1-8192)>**

no lldp tx-delay

Mode Global Configuration Mode

Default 2 seconds

Note: This command executes only if lldp is started

Example

```
Your Product(config)# lldp tx-delay 120
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp` - Displays LLDP global configuration details
- `lldp holdtime-multiplier` – Sets the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP.

lldp notification-interval

Command Objective This command sets the time interval in which the local system generates a notification-event. In the specific interval, generating more than one notification-event is not possible. The value ranges between 5 and 3600 seconds.

The no form of the command sets the notification interval to the default value.

Syntax **lldp notification-interval <seconds(5-3600)>**

no lldp notification-interval

Mode Global Configuration Mode

Default 5 seconds

Note: This command executes only if lldp is started

Example Your Product(config)# lldp notification-interval 150

Related Command(s)

- `show lldp` - Displays LLDP global configuration details
- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.

lldp chassis-id-subtype

Command Objective This command configures an ID for LLDP chassis subtype which is a unique address of any module.

Note: Chassis id value can be set only for the chassis-component and local system subtypes. For all other subtypes, it takes the value from the system automatically.

Syntax **lldp chassis-id-subtype { chassis-comp <string(255)> | if- alias | port-comp <string(255)> | mac-addr | nw-addr | if- name | local <string(255)> }**

Parameter Description

- `chassis-comp <string(255)>` - Represents a chassis identifier based on the value of entPhysicalAlias object for a chassis component
- `if-alias` - Represents a chassis identifier based on the value of ifAlias for an interface on the containing chassis.
- `port-comp <string(255)>` - Represents a chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis
- `mac-addr` - Represents a chassis identifier based on the value of a unicast source address, of a port on the chassis
- `nw-addr` - Represents a chassis identifier based on a network address,associated with a particular chassis. The encoded address is actually composed of two fields. The first field is a single octet, representing the IANA AddressFamilyNumbers value for the specific address type, and the second field is the network address value.
- `if-name` - Represents a chassis identifier based on the value of ifName object for an interface on the containing chassis.
- `local <string(255)>` - Represents a chassis identifier based on a locally defined value."

Mode Global Configuration Mode

Default mac-addr

Note: This command executes only if lldp is started

Example

```
Your Product(config)# lldp chassis-id-subtype chassis-comp
Aricentswitch
Your Product(config)# lldp chassis-id-subtype if-alias
```

Related Command(s)

- `show lldp` - Displays LLDP global configuration details
- `show lldp local` - Displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.
- `no shutdown lldp`– Starts all the ports in the LLDP and releases all the allocated memory.

clear lldp counters

Command Objective This command clears the inbuilt counter which has the total count of LLDP frames that are transmitted/ received.

Note: This command does not clear the global statistics.

Syntax clear lldp counters

Mode Global Configuration Mode

Note: This command executes only if lldp is started

Example `Your Product(config)# clear lldp counters`

Related Command(s)

- `show lldp traffic`- Displays the LLDP counters on all interfaces or on a specific interface
- `no shutdown lldp`– Starts all the ports in the LLDP and releases all the allocated memory.

clear lldp table

Command Objective This command clears all the LLDP information about the neighbors.

Syntax **clear lldp table**

Mode Global Configuration Mode

Note: This command executes only if lldp is started

Example `Your Product(config)# clear lldp table`

Related Command(s)

- `show lldp neighbors` - Displays information about the neighbors on an interface or all interfaces.
- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.

lldp transmit / receive

Command Objective This command transmits or receives LLDP frames from the one of the ports of the server to the LLDP module.

The no form of the command resets LLDP admin status on an interface.

Syntax **lldp {transmit | receive} [mac-address <mac_addr>]**
no lldp {transmit | receive} [mac-address <mac_addr>]

Parameter Description

- **transmit** - Enables transmission of LLDPDU from one of the ports of the server to the LLDP module.
- **receive** - Enables reception of LLDPDU from one of the ports of the server to the LLDP module.
- **mac-address <mac_addr>** - Configures the MAC address to be used as destination MAC address by the LLDP agent on the specified port

Mode Interface Configuration Mode

Default Transmission and Reception are enabled

Note: This command executes only if lldp is started

Example Your Product(config-if)# lldp transmit

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp interface` - Displays LLDP configuration details on a particular interface or all interfaces
- `show lldp statistics` - Displays the LLDP remote table statistics information.

lldp notification

Command Objective This command controls the transmission of LLDP notifications.

The no form of the command disables LLDP trap notification on an interface.

Syntax **lldp notification [remote-table-chg][mis-configuration] [mac-address <mac_addr>]**

no lldp notification [mac-address <mac_addr>]

Parameter Description

- `remote-table-chg` - Sends trap notification to NMS whenever remote table change occurs.
- `mis-configuration` - Sends trap notification to NMS whenever misconfiguration is identified.
- `mac-address <mac_addr>` - Configures the MAC address to be used as destination MAC address by the LLDP agent on the specified port

Mode Interface Configuration Mode

Default mis-configuration

Note: This command executes only if lldp is started

Example

```
Your Product(config-if)# lldp notification remote-table- chg
```

Related Command(s)

- `show lldp interface` - Displays LLDP configuration details on a particular interface or all interfaces
- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.

lldp tlv-select basic-tlv

Command Objective This command enables the basic settings while transmitting the LLDP frames on a given port.

The no form of the command disables the basic TLV transmission on a given port.

Syntax **lldp tlv-select basic-tlv ([port-descr] [sys-name] [sys- descr] [sys-capab] [mgmt-addr {all | ipv4 <ucast_addr> | ipv6 <ip6_addr>}]) [mac-address <mac_addr>]no lldp tlv- select basic-tlv { [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr {all | ipv4 <ucast_addr> | ipv6 <ip6_addr>}] } [mac-address <mac_addr>]**

Parameter Description

- `port-descr` - Configures the port, which is a combination of interface type and interface ID. The interface ID is a combination of slot number and the port number (slot number/port number).
- `sys-name` - Configures the system name of the TLV
- `sys-descr` - Configures the system description of the TLV
- `sys-capab` - Configures the system capabilities of the TLV
- `mgmt-addr` - Enables the transmission on the current interface
  - `all`- Enables the transmission of all the available management addresses on the current interface. If no management address is present/ configured in the system, switch mac-address will be taken for transmission.
  - `ipv4 <ip addr>` - Enables the transmission of a particular ipv4 address on the current interface.
  - `ipv6 <ip addr>` - Enables the transmission of a particular ipv6 address on the current interface.

- mac-address <mac_addr> - Configures the MAC address to be used as destination MAC address by the LLDP agent on the specified port.

  Note: Mac Address can be configured only if LLDP version is set as v2.

Mode Interface Configuration Mode (Physical Interfaces)

Note: This command executes only if; lldp is started in the system

Example

```
Your Product(config-if)# lldp tlv-select basic-tlv port- descr mgmt-addr
all
```

Related Command(s)

- `no shutdown lldp`– Starts all the ports in the LLDP and releases all the allocated memory.
- `set lldp version` - Enables the lldp version to be used on the system
- `show lldp local` – Displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces

lldp port-id-subtype

Command Objective This command configures an ID for LLDP port subtype

Syntax **lldp port-id-subtype { if-alias | port-comp <string(255)> | mac-addr | if-name | local <string(255)> }**

Parameter Description

- `if-alias` - Represents a chassis identifier based on the value of ifAlias for an interface on the containing chassis.
- `port-comp <string(255)>` - Represents a chassis identifier based on the value ofentPhysicalAlias object for a port or backplane within the chassis.
- `mac-addr` - Represents a chassis identifier based on the value of a unicast source address, of a port on the containing chassis.
- `if-name` - Represents a chassis identifier based on the value of ifName object for an interface on the containing chassis.
- `local <string(255)>`- Represents a chassis identifier based on a locally defined value."

Mode Interface Configuration Mode

Default if-alias

Note: This command executes only if lldp is started

Example

```
Your Product(config-if)# lldp port-id-subtype mac-addr
Your Product(config-if)# lldp port-id-subtype local slot0/1
```

Related Command(s)

- `show lldp local` – Displays the current switch information that will be used to populate the outbound LLDP advertisements for a specific interface or all interfaces
- `no shutdown lldp`– Starts all the ports in the LLDP and releases all the allocated memory.

lldp tlv-select dot1tlv

Command Objective This command performs dot1 TLV configuration while transmitting the LLDP frames to the particular port apart from the basic settings.

The no form of the command disables the transmission of dot1 TLV types on a port.

Syntax **lldp tlv-select dot1tlv {[port-vlan-id] [protocol-vlan-id {all |<vlan-id>}] [vlan-name {all | <vlan-id>}][vid-usage- digest] [mgmt-vid] [link-aggregation]}**

no lldp tlv-select dot1tlv {[port-vlan-id] [protocol-vlan- id {all |<vlan-id>}] [vlan-name {all | <vlan-id>}][vid- usage-digest] [mgmt-vid] [link-aggregation]}

Parameter Description

- `port-vlan-id` - Specifies the VLAN ID of the port that uniquely identifies a specific VLAN. This VLAN ID is associated with a specific group of protocols for the specific port.
- `protocol-vlan-id` - Specifies the protocol ID that represents a specific group of protocols that are associated together when assigning a VID to a frame. This group ID is associated with the specific port.
  - `all`**–** Sets the protocol ID as all
  - `<vlan-id>` - Sets the protocol id as the mentioned vlan id. This value ranges between 1 and 4094.
- `vlan-name` - Specifies the administratively assigned string, which is used to identify the VLAN.
  - `all`**–** Sets the protocol ID as all
  - `<vlan-id>` - Sets the protocol id as the mentioned vlan id. This value ranges between 1 and 4094.
- `vid-usage-digest` - Performs dot1 TLV configuration while transmitting the LLDP frames to the VID usage digest TLV

  Note: This parameter can be set only when LLDP version is set as v2

- `mgmt-vid` - Performs dot1 TLV configuration while transmitting the LLDP frames to the managemet VID TLV

  Note: This parameter can be set only when LLDP version is set as v2

- `link-aggregation` - Performs dot1 TLV configuration while transmitting the LLDP frames to the link-aggregation TLV

Note: This parameter can be set only when LLDP version is set as v2

Mode Interface Configuration Mode

Note: This command executes only if lldp is started

Example

```
Your Product(config-if)# lldp tlv-select dot1tlv port- vlan-id protocol-
vlan-id 42
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp neighbors` - Displays information about the neighbors on an interface or all interfaces.
- `show lldp local` – Displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces
- `show lldp errors` - Displays the information about the errors such as memory allocation failures, queue overflows and table overflow.
- `set lldp version` - Enables the lldp version to be used on the ports.

lldp tlv-select dot3tlv

Command Objective This command performs dot3 TLV configuration while transmitting the LLDP frames to the particular port apart from the basic settings.

The no form of the command disables the transmission of dot3 TLV types on a port.

Syntax **lldp tlv-select dot3tlv { [macphy-config] [link- aggregation] [max-framesize] }**

no lldp tlv-select dot3TLV { [macphy-config] [link- aggregation] [max-framesize] }

Parameter Description

- `macphy-config` - Configures the physical MAC address of the TLV.
- `link-aggregation` - Configures the link aggregation protocol statistics for each port on the device.
- `max-framesize` - Configures the maximum frame size of the TLV.

Mode Interface Configuration Mode

Note: This command executes only if lldp is started

Example Your Product(config-if)# lldp tlv-select dot3tlv macphy- config

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp neighbors` - Displays information about the neighbors on an interface or all interfaces.
- `show lldp local` – Displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces

- `show lldp errors` - Displays the information about the errors such as memory allocation failures, queue overflows and table overflow.

debug lldp

Command Objective This command specifies debug level for LLDP module.

The no form of the command disables debug option for LLDP module.

Syntax **debug lldp [{all | [init-shut] [mgmt] [data-path] [ctrl] [pkt-dump] [resource] [all-fail] [buf] [neigh] [critical][tlv {all | [chassis-id][port-id] [ttl] [port- descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr] [port-vlan] [ppvlan] [vlan-name] [proto-id] [mac-phy] [pwr-mdi] [lagg] [max-frame] [vid-digest] [mgmt-vid] [dcbx-cee]}] [redundancy]}]**

no debug lldp [{all | [init-shut] [mgmt] [data-path] [ctrl] [pkt-dump] [resource] [all-fail] [buf] [neigh] [critical][tlv {all | [chassis-id][port-id] [ttl] [port- descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr] [port-vlan] [ppvlan] [vlan-name] [proto-id] [mac-phy][pwr-mdi] [lagg] [max-frame] [vid-digest] [mgmt-vid] [dcbx-cee]}] [redundancy]}]

Parameter Description

- `all` - Generates debug statements for all traces
- `init-shut` - Generates debug statements for init and shutdown traces. This trace is generated on failed initialization and shutting down of LLDP related entries.
- `mgmt` - Generates debug statements for management traces. This trace is generated during failure in configuration of any of the LLDP features.
- `data-path` - Generates debug statements for data path traces. This trace is generated during failure in packet processing.
- `ctrl` - Generates debug statements for control path traces. This trace is generated during failure in modification or retrieving of LLDP entries
- `pkt-dump` - Generates debug statements for packet dump traces. This trace is currently not used in LLDP module.
- `resource` - Generates debug statements for OS resource related traces. This trace is generated during failure in message queues.
- `all-fail` - Generates debug statements for all failure traces of the above mentioned traces
- `buf` - Generates debug statements for LLDP buffer related traces. This trace is currently not used in LLDP module.
- `neigh` - Generates debug statements for neighbor SEM.
- `critical` - Generates debug statements for critical SEM.
- `tlv` – Generates debug statements for the following traces;
  - `all` - Generates debug statements for all TLV traces
  - `chassis-id` - Generates debug statements for chassis-id TLV traces
  - `port-id` - Generates debug statements for port-id TLV trace
  - `ttl` - Generates debug statements for TTL TLV trace

  - `port-descr` - Generates debug statements for the port description TLV traces
  - `sys-name` - Generates debug statements for the system name TLV traces
  - `sys-descr` - Generates debug statements for system description TLV traces
  - `sys-capab` - Generates debug statements for system capabilities TLV traces
  - `mgmt-addr` - Generates debug statements for management address TLV traces
  - `port-vlan` - Generates debug statements for port-vlan TLV traces
  - `ppvlan` - Generates debug statements for port-protocol-vlan TLV traces
  - `vlan-name` - Generates debug statements for vlan-name TLV traces
  - `proto-id` - Generates debug statements for protocol-id TLV traces
  - `mac-phy` - Generates debug statements for MAC or PHY TLV traces
  - `pwr-mdi` - Generates debug statements for power-through-MDI TLV traces
  - `lagg` - Generates debug statements for link aggregation TLV traces
  - `max-frame` - Generates debug statements for maximum frame size TLV traces
  - `vid-digest` - Generates debug statements for vid digest TLV traces
  - `mgmt-vid` - Generates debug statements for management VID TLV traces
  - `dcbx-cee` - Generates debug statements for dcbx (cee) TLV traces
- `redundancy` - Generates the debug statements for the LLDP redundancy module.

Mode Privileged Exec Mode

Note: This command executes only if lldp is started

Example

```
Your Product# debug lldp init-shut mgmt
Your Product# debug lldp tlv sys-descr lagg
Your Product# debug lldp
```

Related Command(s) `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.

show lldp

Command Objective This command displays LLDP global configuration details to initialize on an interface.

Syntax show lldp

Mode Privileged EXEC Mode

Note: This command executes only if lldp is started

Example

```
Your Product# show lldp
LLDP is enabled
LLDP Version          : v2
Transmit Interval     : 20
```

```
Holdtime Multiplier : 4
Reinitialization Delay     : 2
Tx Delay      : 2
Notification Interval      : 30
TxCreditMax          : 5
MessageFastTx        : 1
TxFastInit    : 4
Chassis Id SubType   : Chassis Component
Chassis Id    : Aricentswitch
```

Related Command(s)

- `set lldp` - Enables or disables LLDP on the system.
- lldp transmit-interval – Sets the transmission interval
- lldp holdtime-multiplier - Sets the multiplier value
- lldp reinitialization-delay - Sets the reinitialization delay
- lldp tx-delay - Sets the transmit delay
- lldp notification-interval - Sets the notification interval
- lldp chassis-id-subtype - Configures lldp chassis id subtype and chassis id value
- no shutdown lldp – Starts all the ports in the LLDP and releases all the allocated memory.
- set lldp version – Enables the lldp version to be used on the system.
- lldptxCreditMax – Configures the maximum number of consecutive LLDPDUs that can be transmitted any time
- lldp MessageFaxtTx – Configures the interval at which LLDP frames are transmitted on behalf of this LLDP agent during fast transmission period
- lldp txFastInit - Configures the value used to initialize the txFast variable which determines the number of transmissions that are made in fast transmission mode

show lldp interface

Command Objective This command displays the information about interfaces where LLDP is enabled.

Syntax **show lldp interface [<interface-type> <interface-id>] [mac-address <mac_addr>]**

Parameter Description

- `<interface-type>` - Displays the information about the specified type of interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer upto 40-Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1-Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10-Gigabits per second. This Ethernet supports only full duplex links.
  - `port-channel` – Logical interface that represents an aggregator which contains several

ports aggregated together.

- <interface-id> - Displays the information about the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. ForExample: 1 represents port-channel ID.
- mac-address <mac_addr> - Displays information about neighbors for the specidfied destination MAC address of the LLDP agent

Mode Privileged EXEC Mode

Note: This command executes only if lldp is started.

Example

```
Your Product# show lldp interface gigabitethernet 0/1
Gi0/1:
Tx State            : Enabled
Rx State      : Enabled
Tx SEM State        : INITIALIZE
Rx SEM State        : INITIALIZE Notification Status : Disabled
Notification Type  : Mis-configuration
DestinationMacAddr  : 01:80:c2:00:00:0e
```

Related Command(s)

- set lldp - Enables or disables LLDP on the system
- lldp transmit / receive - Sets LLDP admin status on an interface to Transmit or Receive
- lldp notification - Enables LLDP trap notification on an interface
- no shutdown lldp – Starts all the ports in the LLDP and releases all the allocated memory.
- lldp dest-mac - Configures destination mac-address to be used by the LLDP agent for transmission on this port.

show lldp neighbors

Command Objective This command displays information about neighbors on an interface or all interfaces.

Syntax **show lldp neighbors [chassis-id <string(255)> port-id <string(255)>] [<interface-type> <interface-id>][detail]**

Parameter Description

- chassis-id <string(255)> - DisplaysLLDP Neighbor information for the specified chassis identifier value This value is a string value with a maximum size of 255.
- port-id <string(255)> - DisplaysLLDP Neighbor information for the specified port number that represents the concerned aggregation port. This value is a string value with a maximum size of 255.

- `<interface-type>` - Displays information about neighbors for the specified type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Displays information about neighbors for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Onl port-channel ID is provided, for interface type port-channel. For example: 1 represents port-channel ID.
- `detail` - Displays the information obtained from all the received TLVs .

Mode Privileged EXEC Mode

Note: This command can be executed only if lldp is started

Example

```
Your Product# show lldp neighbors
Capability Codes  :
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable
Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Chassis ID              Local Intf      Hold-time    Capability   Port Id
----------              ----------      ---------    ----------   -------
00:01:02:03:04:01       Gi0/1           120          B,R          Slot0/1
00:02:02:03:04:01       Gi0/2           120                       Slot0/3
00:02:02:03:04:01       Gi0/3           120                       Slot0/2
00:01:02:03:04:01       Gi0/2           120                       Slot0/2
00:01:02:03:04:01       Gi0/3           120                       Slot0/2
Total Entries Displayed : 5
Your Product# show lldp neighbors chassis-id
00:01:02:03:04:01 port-id Slot0/2
Capability Codes  :
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable
Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Chassis ID              Local Intf      Hold-time    Capability   Port Id
----------              ----------      ---------    ----------   -----
00:01:02:03:04:01       Gi0/2           120                       Slot0/2
00:01:02:03:04:01       Gi0/3           120                       Slot0/2
Total Entries Displayed : 2
Your Product# show lldp neighbors chassis-id
00:01:02:03:04:01 port-id Slot0/2 gigabitethernet 0/2
Capability Codes  :
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable
Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Chassis ID              Local Intf      Hold-time    Capability    Port Id
----------              ----------      ---------    ----------    -----
00:01:02:03:04:01       Gi0/2           120                        Slot0/2
Total Entries Displayed : 1
Your Product# show lldp neighbors chassis-id
00:01:02:03:04:01 port-id Slot0/2 detail
Capability Codes  :
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable
Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Chassis Id SubType            : Mac Address
Chassis Id                    : 00:01:02:03:04:01
Port Id SubType               : Interface Alias
Port Id                       : Slot0/2
Port Description              : Not Advertised
System Name                   : Not Advertised
System Desc                   : Not Advertised
Local Intf                    : Gi0/2
Time Remaining                : 92 Seconds
System Capabilities Tlv       : Not Advertised
Management Addresses          : Not Advertised
Extended 802.3 TLV Info
-MAC PHY Configuration & Status
Auto Negotiation Tlv          : Not Advertised
-Link Aggregation
Link Aggregation Tlv          : Not Advertised
-Maximum Frame Size Tlv       : Not Advertised
Extended 802.1 TLV Info
-Port VLAN Id                 : 0
-Port & Protocol VLAN Id
Protocol Vlan Tlv             : Not Advertised
-Vlan Name
Vlan Id       Vlan Name
-------       ---------
------------------------------------------------------------
Chassis Id SubType            : Mac Address
Chassis Id                    : 00:01:02:03:04:01
Port Id SubType               : Interface Alias
Port Id                       : Slot0/2
Port Description              : Not Advertised
System Name                   : Not Advertised
System Desc                   : Not Advertised
Local Intf                    : Gi0/3
Time Remaining                : 92 Seconds
System Capabilities Tlv       : Not Advertised
Management Addresses          : Not Advertised
Extended 802.3 TLV Info
-MAC PHY Configuration & Status
Auto Negotiation Tlv          : Not Advertised
-Link Aggregation
Link Aggregation Tlv          : Not Advertised
-Maximum Frame Size Tlv       : Not Advertised
Extended 802.1 TLV Info
-Port VLAN Id                 : 0
```

```
-Port & Protocol VLAN Id
Protocol Vlan Tlv            : Not Advertised
-Vlan Name
Vlan Id       Vlan Name
-----------   --------------
------------------------------------------------------------------------------------------
Total Entries Displayed : 2
Your Product# show lldp neighbors gigabitethernet 0/1 detail
Capability Codes  :
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable
Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Chassis Id SubType            : Mac Address
Chassis Id                    : 00:01:02:03:04:01
Port Id SubType               : Interface Alias
Port Id                       : Slot0/1
Port Description              : Ethernet Interface
System Name                   : SMIS
System Desc                   : SNMPV2
Local Intf                    : Gi0/1
Time Remaining                : 95 Seconds
System Capabilities Supported : B,R
System Capabilities Enabled   : B,R
Management Addresses          :
IfId SubType Address                        OID
---- ------- -------                        ---
33  IPv4   12.0.0.1                   1 3 6 1 2 1 2 2 1
1
Extended 802.3 TLV Info
-MAC PHY Configuration & Status
Auto-Neg Support & Status    : Supported, Disabled
Advertised Capability Bits   : 8000
Other
-Link Aggregation
Capability & Status          : Not Capable, Not In
Aggregation
Aggregated Port Id           : 1
-Maximum Frame Size          : 1500
Extended 802.1 TLV Info
-Port VLAN Id                : 1
-Port & Protocol VLAN Id
Protocol Vlan Id        Support         Status
------------------------ ----------- ----------
1                       Supported       Enabled
2                       Supported       Enabled
30                      Supported       Enabled
-Vlan Name
Vlan Id       Vlan Name
-----------   --------------
1             vlan1
2             vlan2
30            vlan30
------------------------------------------------------------------------------------------
Total Entries Displayed : 1
```

Related Command(s)

- no shutdown lldp – Starts all the ports in the LLDP and releases all the allocated memory.
- set lldp - Enables or disables LLDP on the system
- clear lldp table - Clears all the LLDP table of information about the neighbors.
- lldp tlv-select basic-tlv – Configures basic TLV types to be transmitted on a given port
- lldp tlv-select dot1tlv – Configures dot1 TLV types to be transmitted on a port
- lldp tlv-select dot3tlv - Configures dot3 TLV types to be transmitted on a port

show lldp traffic

Command Objective This command displays LLDP counters on all interfaces or on a specific interface. This includes the following:

- Total Frames Out
- Total Entries Aged
- Total Frames In
- Total Frames Received In Error
- Total Frames Discarded
- Total TLVS Unrecognized
- Total TLVs Discarded

Syntax **show lldp traffic [<iftype> <ifnum>[mac-address <mac_addr>]]**

Parameter Description

- <iftype> - Displays the LLDP counters for specified type of interface. Th interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- <ifnum> - Displays the LLDP counters for specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. ForExample: 1 represents port-channel ID
- mac-address <mac_addr> - Displays information about neighbors for the specidfied destination MAC address of the LLDP agent

Mode Privileged EXEC Mode

Note: This command executes only if lldp is started

Example

```
Your Product# show lldp traffic
Total Frames Out                 : 107
Total Entries Aged               : 0
Total Frames In                  : 159
Total Frames Received In Error : 0
Total Frames Discarded           : 0
Total TLVS Unrecognized          : 0
Total TLVs Discarded             : 0
Your Product# show lldp traffic gigabitethernet 0/1
Total Frames Out                 : 49
Total Entries Aged               : 0
Total Frames In                  : 42
Total Frames Received In Error : 0
Total Frames Discarded           : 0
Total TLVS Unrecognized          : 0
Total TLVs Discarded             :  0
Total  PDU  length  error  Drops  :  0
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `set lldp` - Enables or disables LLDP on the system
- `clear lldp counters` - Clears the entire interface related transmit and receive counters.

show lldp local

Command Objective This command displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.

Syntax **show lldp local {[<interface-type> <interface-id> [mac- address <mac_addr>]] | [mgmt-addr]}**

Parameter Description

- `<interface-type>` - Displays the current switch information for the specified type of interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.

    - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together

- `<interface-id>` - Displays the current switch information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel.For example: 1 represents port-channel ID.
- `mac-address <mac_addr>` - Displays information about neighbors for the specidfied destination MAC address of the LLDP agent.
- `mgmt-addr` - All the management addresses configured in the system and Tx enabled ports.

Mode Privileged EXEC Mode

Note: This command can be executed only if lldp is started

Example

```
Your Product# show lldp local

Capability Codes  :
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable
Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Chassis Id SubType                 : Mac Address
Chassis Id                         : 00:02:02:03:04:01
System Name                        : SMIS
System Description                 : SNMPV2
System Capabilities Supported      : B,R
System Capabilities Enabled        : B,R
Gi0/1                              :
Port Id SubType                    : Interface Alias
Port Id                            : Gi0/1
Port Description                   : Ethernet Interface Port 01
Enabled Tx Tlvs                    : Port Description, System
Description,
Management Address
Extended 802.3 TLV Info
-MAC PHY Configuration & Status
Auto-Neg Support & Status          : ,
Advertised Capability Bits         : b24e
Other
10base-T(FD)
100base-T4
100base-T2(HD) Asym PAUSE(FD)
1000base-X, -LX, -SX, -CX(HD)
1000base-X, -LX, -SX, -CX(FD)
1000base-T(HD)
Operational MAU Type       : 0
-Link Aggregation
Capability & Status        : Not Capable, Not In
Aggregation
```

```
Aggregated Port Id                 : 0
-Maximum Frame Size                : 1500
Extended 802.1 TLV Info
-Port VLAN Id                      : 1
-Port & Protocol VLAN Id
Protocol VLAN Id        Support         Protocol VLAN Status             TxStatus
----------------        ----------      --------------------             --------
0                       Supported       Enabled                          Disabled
1                       Supported       Enabled                          Disabled
-Vlan Name
Vlan Id                 Vlan Name                                        TxStatus
----------              ----------                                       --------
1                                                                        Disabled
-VID TLV:
VID                     TxStatus
-------                 ----------
0                       Disabled
-Management             Vid TLV:
Vlan Id                 TxStatus
-------                 ----------
1                       Disabled
--------------------------------------------------------------------------------
Your Product# show lldp local gigabitethernet 0/1
Port Id SubType                    : Interface Alias
Port Id                            : Slot0/1
Port Description                   : Ethernet Interface
Enabled Tx Tlvs                    : Port Description, System Name,
                                   System Description, System Capability,
                                   Management Address, Port Vlan, Mac
Phy,

Extended 802.3 TLV Info
-MAC PHY Configuration & Status

Link Aggregation, Max Frame Size
Auto-Neg Support & Status          : Supported, Disabled
Advertised Capability Bits         : 8000
Other
Operational MAU Type               : 0
-Link Aggregation
Capability & Status                : Not Capable, Not In
Aggregation
Aggregated Port Id                 : 1
-Maximum Frame Size                : 1500
Extended 802.1 TLV Info
-Port VLAN Id                      : 1
-Port & Protocol VLAN Id
Protocol VLAN Id        Support         Protocol VLAN Status       TxStatus
----------------        -----------     -----------------------------------
-
1                       Supported       Enabled                    Enabled
2                       Supported       Enabled                    Enabled
30                      Supported       Enabled                    Enabled
-Vlan Name
Vlan Id                   Vlan Name                          TxStatus
-------------           -----------                          ---------------
```

```
--------------------------          ----------------------                ------------------------------
1                                vlan1                                 Enabled
2                                vlan2                                 Enabled
30                               vlan3                                 Enabled
---------------------------------------------------------------------------------------------------------------
Your Product# show lldp local mgmt-addr
Management Address                 TxEnabledPorts
----------------------------       ---------------------
13.0.0.1                           Gi0/1
15.0.0.1                           Gi0/1
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `set lldp` - Enables or disables LLDP on the system
- `lldp chassis-id-subtype` - Configures lldp chassis id subtype and chassis id value
- `lldp port-id-subtype` - Configures lldp port id subtype and port id value for a given port
- `lldp tlv-select basic-tlv` – Configures basic TLV types to be transmitted on a given port
- `lldp tlv-select dot1tlv` – Configures dot1 TLV types to be transmitted on a port
- `lldp tlv-select dot3tlv` – Configures dot3 TLV types to be transmitted on a port

show lldp errors

Command Objective This command displays the information about the errors such as memory allocation failures, queue overflows and table overflow.

Syntax **show lldp errors**

Mode Privileged EXEC Mode

Example

```
Your Product# show lldp errors
Total Memory Allocation Failures : 0
Total Input Queue Overflows : 0 Total
Table Overflows                  : 0
```

Note: This command can be executed only if lldp is started

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `set lldp` - Enables or disables LLDP on the system
- `lldp tlv-select basic-tlv` – Configures basic TLV types to be transmitted on a given port
- `lldp tlv-select dot1tlv` – Configures dot1 TLV types to be transmitted on a port
- `lldp tlv-select dot3tlv` - Configures dot3 TLV types to be transmitted on a port

show lldp statistics

Command Objective This command displays the LLDP remote table statistics information.

Syntax **show lldp statistics**

Mode Privileged EXEC Mode

Example

```
Your Product# show lldp statistics
Remote Table Last Change Time : 100300
Remote Table Inserts         : 5
Remote Table Deletes         : 0
Remote Table Drops           : 0
Remote Table Ageouts         : 0
Remote Table Updates         : 4
```

Note: This command can be executed only if lldp is started

Related Command(s)

- `set lldp` - Enables or disables LLDP on the system
- `lldp transmit / receive` - Sets LLDP admin status on an interface to transmit / receive
- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.

lldp dest-mac

Command Objective This command configures destination mac-address to be used by the LLDP agent for transmission on this port.

The no form of the command resets the destination mac-address to LLDP multicast address .

Syntax **lldp dest-mac <mac_addr>**

no lldp dest-mac <mac_addr>

Mode Interface Configuration Mode (Physical Interfaces)

Default The default value would the LLDP multicast MAC address

Note: This command can be executed only if lldp is started.

Example

```
Your Product(config-if)# lldp dest-mac 00:11:22:33:44:55
```

Related Command(s)

- `no shutdown lldp` – . Enables all the ports by allocating the required resources in the LLDP.
- `show lldp interface` - Displays the information about interfaces where LLDP is enabled

set lldp version

Command Objective This command enables the lldp version to be used on the system.

Syntax **set lldp version {v1 | v2}**

Parameter Description

- `v1` - Enables LLDP 2005 version 1 on the port
- `v2` - Enables LLDP 2009 version 2 on the port

Mode Global Configuration Mode

Default v1

Note: This command executes only if lldp is started

Example

```
Your Product(config)# set lldp version v1
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp` - Displays LLDP global configuration details to initialize on an interface

lldp txCreditMax

Command Objective This command configures the maximum number of consecutive LLDPDUs that can be transmitted any time. This value ranges between 1 and 10.

Syntax **lldp txCreditMax <value (1-10)>**

Mode Global Configuration Mode

Default 5

Note: This command executes only if lldp is started

Example

```
Your Product(config)# lldp txCreditMax 3
```

Related Command(s)

- no shutdown lldp – Starts all the ports in the LLDP and releases all the allocated memory.
- show lldp - Displays LLDP global configuration details to initialize on an interface

lldp MessageFastTx

Command Objective This command configures the interval at which LLDP frames are transmitted on behalf of this LLDP agent during fast transmission period. This value ranges between 1 and 3600 seconds.

Syntax lldp MessageFastTx <seconds(1-3600)>

Mode Global Configuration Mode

Default 1

Note: This command executes only if lldp is started

Example `Your Product(config)# lldp MessageFastTx 3500`

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp` - Displays LLDP global configuration details to initialize on an interface

lldp txFastInit

Command Objective This command configures the value used to initialize the txFast variable which determines the number of transmissions that are made in fast transmission mode. This value ranges between 1 and 8.

Syntax **lldp txFastInit <value (1-8)>**

Mode Global Configuration Mode

Default 4

Note: This command executes only if lldp is started

Example `Your Product(config)# lldp txFastInit 3`

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `show lldp` - Displays LLDP global configuration details to initialize on an interface

show lldp peer

Command Objective This command displays information about the peers on an interface or all interfaces.

Syntax **show lldp peers [chassis-id <string(255)> port-id <string(255)>] <interface-type> <interface-id>[[mac-address <mac_addr>] [detail]]**

Parameter Description

- `chassis-id <string(255)>` - Displays the LLDP peer information for the specified chassis identifier. This value is a string of maximum size 255.
- `port-id <string(255)>` - Displays the port number that represents the concerned aggregation port This value is a string of maximum size 255.

- `<interface-type>` - Displays information about LLDP peers for the specified type of interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Displays information about peers for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For example: 1represents port-channel ID.
- `mac-address <mac_addr>` - Displays information about peers for the specidfied destination MAC address of the LLDP agent
- `detail` - Displays the information obtained from all the received TLVs .

Mode Privileged EXEC Mode

Note: This command can be executed only if lldp is started

Example `Your Product # show lldp peers gigabitethernet 0/1`

```
Capability Codes          :

 (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable

Device,

 (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Chassis ID        Local Intf       Hold-time       Capability       Port Id

-------           -------          ------          -------          -----

00:01:02:03:04:01 Gi0/1            120             B,R              Slot0/1
```

Related Command(s)

- `no shutdown lldp` – Starts all the ports in the LLDP and releases all the allocated memory.
- `set lldp` - Enables or disables LLDP on the system
- `clear lldp table` - Clears all the LLDP table of information about the neighbors.
- `lldp tlv-select basic-tlv` – Configures basic TLV types to be transmitted on a given port
- `lldp tlv-select dot1tlv` – Configures dot1 TLV types to be transmitted on a port
- `lldp tlv-select dot3tlv` - Configures dot3 TLV types to be transmitted on a port

20 VLAN

VLANs (Virtual LANs) can be viewed as a group of devices on different physical LAN segments which can communicate with each other as if they were all on the same physical LAN segment, that is, a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which make them extremely flexible.

VLAN provides the following benefits for switched LANs:

- Improved administration efficiency
- Optimized Broadcast/Multicast Activity
- Enhanced network security

The prompt for the switch configuration mode is,

Your Product(config)#
The prompt for the Config VLAN mode is,

Your Product(config-vlan)#

The list of commands for the configuration of VLAN is as follows:

- shutdown vlan
- vlan
- set mac-learning
- base bridge-mode
- mac-vlan
- subnet-vlan
- protocol-vlan
- map protocol
- set vlan traffic-classes
- mac-address-table static unicast – Transparent Bridging Mode
- mac-address-table static multicast
- mac address-table static mcast
- mac-address-table static multicast – Transparent Bridging mode
- mac-address-table aging-time
- clear vlan statistics
- wildcard
- unicast-mac learning limit
- map subnet
- ports
- vlan active
- set unicast-mac learning

- interface range
- vlan unicast-mac learning limit
- switchport pvid
- switchport access vlan
- switchport acceptable-frame-type
- switchport ingress-filter
- protocol-vlan
- switchport map protocols-group
- switchport priority default
- switchport mode
- vlan max-traffic-class
- vlan map-priority
- mac-map
- switchport filtering-utility-criteria
- switchport protected
- debug vlan
- show vlan
- show vlan device info
- show vlan device capabilit ies
- show vlan traffic-classes
- show vlan port config
- show vlan protocols-group
- show protocol-vlan
- show mac-vlan
- show subnet vlan mapping
- show vlan statistics
- show vlan learning params
- show mac-address-table
- show dot1d mac-address-table
- show mac-address-table count
- show mac-address-table static unicast
- show dot1d mac-address-table static unicast
- show mac-address-table static multicast
- show dot1d mac-address-table static multicast
- show mac-address-table dynamic unicast
- show mac-address-table dynamic multicast
- show mac-address-table aging-time
- show wildcard
- shutdown garp
- set gvrp
- set port gvrp
- set port gvrp - enable | disable
- set gmrp

- set port gmrp
- set garp timer
- vlan restricted
- group restricted
- debug garp
- show garp timer
- switchport unicast-mac learning
- private-vlan
- private-vlan association
- switchport private-vlan host-association
- switchport private-vlan mapping
- show vlan private-vlan
- set filtering-utility-criteria
- set sw-stats
- set vlan counter
- clear mac-address-table dynamic
- debug vlan global
- show gmrp statistics
- show gvrp statistics

shutdown vlan

Command Objective This command shuts down the VLAN switching feature in the switch and releases all resources allocated to the VLAN feature.

The no form of the command starts and enables VLAN switching feature in the switch. The resources required for the VLAN feature are also allocated to it.

The VLAN feature allows you to logically segment a shared media LAN for forming virtual workgroups.

Syntax **shutdown vlan**

no shutdown vlan

Mode Global Configuration Mode

Default VLAN switching feature is started and enabled in the switch.

Notes:

- VLAN module can be shutdown, only if the GARP module is shutdown.
- VLAN switching configuration is not allowed in the switch, if the base bridge mode is set as transparent bridging.

Example

```
Your Product(config)# shutdown vlan
```

Related Command(s)

- `set vlan` - Globally enables / disables VLAN feature in the switch (that is the status of the VLAN feature is configured for all ports of the switch).
- `vlan` - Creates a VLAN in the ISS and enters into the config-VLAN mode in which VLAN specific configurations are done.
- `base bridge-mode` - Configures the base mode (either 802.1d transparent bridge mode or 802.1q vlan aware bridge mode) in which the VLAN feature should operate on the switch.
- `mac-vlan` - Enables MAC-based VLAN membership classification on all ports of the switch.
- `subnet-vlan` - Enables subnet-VLAN based membership classification on all ports of the switch.
- `protocol-vlan` - Enables protocol-VLAN based membership classification on all ports of the switch.
- `map protocol` - Creates a protocol group with a specific protocol and encapsulation frame type combination.
- `set gvrp` – Globally enables / disables GVRP feature on all ports of a switch.
- `set gmrp` – Globally enables / disables GMRP feature on all ports of a switch.
- `set vlan traffic-classes` - Enables or disables traffic class feature in a switch on all ports.
- `mac-map` - Configures the VLAN-MAC address mapping that is used only for MAC-based VLAN membership classification.
- `map subnet` - Configures VLAN-IP subnet address mapping that is used only for subnet-VLAN based membership classification.
- `switchport filtering-utility-criteria` - Creates filtering utility criteria for the port.
- `switchport protected` - Enables switchport protection feature for a port.
- `mac-address-table aging-time` - Configures the timeout period (in seconds) for aging out dynamically learned forwarding information entry and static entry in the MAC address table.
- `clear vlan statistics` - Clears VLAN counters that maintain statistics information on a per VLAN basis. The counter is cleared for all available VLANs or for the specified VLAN.
- `vlan default hybrid type` - Configures the default hybrid learning mode for all VLANs when the operational learning mode of the switch is globally set as hybrid.
- `wildcard` - Configures the wildcard VLAN entry for a specified MAC address or any MAC address.
- `unicast-mac learning limit` - Configures the unicast-MAC learning limit for a switch.
- `switchport pvid` - Configures the PVID on the specified port.
- `switchport acceptable-frame-type` – Configures the type of VLAN dependant BPDU frames such as GMRP BPDU, that the port should accept during the VLAN membership configuration.
- `switchport ingress-filter` - Enables ingress filtering feature on the port.
- `port protocol-vlan` - Enables protocol-VLAN based membership classification in a port.
- `switchport map protocols-group` - Maps the configured protocol group to a particular VLAN ID for an interface.
- `switchport priority default` - Configures the default ingress user priority for a port.
- `switchport mode` - Configures the mode of operation for a switch port.
- `vlan max-traffic-class` - Configures the maximum number of traffic classes supported on a port.
- `vlan map-priority` - Maps an evaluated user priority to a traffic class on a port.
- `shutdown garp` - Shuts down the GARP module in the switch on all ports and releases all

memories used for the GARP module.

- `debug vlan` - Enables the tracing of the VLAN submodule as per the configured debug levels.
- `show vlan` - Displays VLAN entry related information of all active VLANs and VLANs (that are not active) for which the port details are configured.
- `show vlan device info` - Displays the VLAN global information that is applicable to all VLANs created in the switch / all contexts.
- `show vlan device capabilities` - Displays only the list of VLAN features such as traffic class feature, supported in the switch / all contexts.
- `show vlan traffic-classes` - Displays the evaluated user priority and traffic class mapping information of all interfaces available in the switch / all contexts.
- `show garp timer` - Displays the GARP timer information of all interfaces available in the switch / all contexts.
- `show vlan port config` - Displays the VLAN related port specific information for all interfaces available in the switch / all contexts.
- `show vlan protocols-group` - Displays all entries in the protocol group table.
- `show protocol-vlan` - Displays all entries in the port protocol table.
- `show mac-vlan` - Displays all entries in the MAC map table.
- `show subnet-vlan mapping` - Displays all entries in the subnet map table.
- `show vlan statistics` - Displays the unicast / broadcast statistics details of all active VLANs and VLANs (that are not active) for which the port details are configured.
- `show mac-address-table` - Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table.
- `show dot1d mac-address-table` - Displays all static / dynamic unicast and multicast MAC address entries created in the FDB table, when the VLAN base bridge mode is transparent bridging.
- `show dot1d mac-address-table static unicast`- Displays all static unicast MAC address entries created in the FDB table, when the VLAN base bridge mode is transparent bridging.
- `show dot1d mac-address-table static multicast` - Displays all static multicast MAC address entries created in the FDB table, when the VLAN base bridge mode is transparent bridging.
- `show mac-address-table count` - Displays the total number of static / dynamic unicast and multicast MAC address entries created in the FDB table.
- `show mac-address-table static unicast` - Displays all static unicast MAC address entries created in the FDB table.
- `show mac-address-table static multicast` - Displays the static multicast MAC
- address entries created in the FDB table.
- `show mac-address-table dynamic unicast` - Displays all dynamically learnt unicast entries from the MAC address table.
- `show mac-address-table dynamic multicast` - Displays all dynamically learnt multicast entries from the MAC address table.
- `show mac-address-table aging-time` - Displays the ageing time configured for the MAC address table.
- `show wildcard` - Displays all wildcard MAC entries created in the switch / in all contexts.
- `show vlan learning params` - Displays the VLAN learning parameter details for all active VLANs and VLANs (that are not active) for which the port details are configured, available in all contexts /

in the switch.

vlan

Command Objective This command creates a VLAN / VFI ID and enters into the config-VLAN mode in which VLAN specific configurations are done. This command directly enters into the config-VLAN mode for the specified VLAN / VFI ID, if the VLAN is already created.

- `<vlan -id>` - This is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
- `<vfi-id>.` - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This feature is not available in SMIS switch models.
    - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
    - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

The no form of the command deletes the existing VLAN/ VFI and its corresponding configurations.

Syntax **vlan <vlan-id/vfi_id>**

no vlan <vlan-id/vfi_id>

Mode Global Configuration Mode

Default By default VLAN 1 is created

Notes:

- The Native VLAN (VLAN 1) created by default cannot be deleted using the no form of the command.
- For default VLAN 1, interface VLAN configuration alone is permitted and no other configuration on this VLAN is allowed, if the base bridge mode is set as transparent bridging. No new VLAN can be created, if the base bridge mode is set as transparent bridging
- The creation of new VLAN and configuration of existing VLAN can be done, only if the VLAN switching feature is started and enabled in the switch.

Example

```
Your Product(config)# vlan 4Your

Product(config-vlan)#
```

Related Command(s)

- `base bridge-mode` - Configures the base mode (either 802.1d transparent bridge mode or 802.1q vlan aware bridge mode) in which the VLAN feature should operate on the switch.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `interface vlan <vlan-id>` - Creates an L3 VLAN interface. An L3 VLAN interface is a VLAN that is mapped to an IP interface and assigned an IP address.
- `show vlan` - Displays VLAN entry related information of all active VLANs and VLANs (that are not active) for which the port details are configured.

set mac-learning

Command Objective This command configures the global mac learning status.

Syntax **set mac-learning { enable | disable }**

Parameter Description

- `enable` - Enables the global mac learning status
- `disable` - Disables the global mac learning status

Mode Global Configuration Mode

Default enable

Example

```
Your Product(config)# set mac-learning enable
```

base bridge-mode

Command Objective This command configures the base mode (either 802.1d transparent bridge mode or 802.1q vlan aware bridge mode) in which the VLAN feature should operate on the switch. This configuration is globally applied on all ports of the switch.

Syntax **base bridge-mode { dot1d-bridge | dot1q-vlan }**

Parameter Description

- `dot1d-bridge` - Configures the VLAN operation mode as transparent bridging. The switch operates according to IEEE 802.1q implementation. This mode allows you to connect two similar network segments to each other at the datalink layer in a manner transparent to end stations, so the end stations do not participate in the bridging algorithm.

  The mode can be set as transparent bridging, only if the following conditions are satisfied:

  - GARP, IGS, MLDS, LA, and LLDP are shutdown.
  - Spanning tree mode is set as RSTP or spanning tree is shutdown.
  - All logical interfaces such as loopback, are deleted. The default L3 VLAN interface is also deleted.

- `dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging. The switch operates according to IEEE 802.1d implementation. This mode allows you to interconnect end stations at different LAN segments and communicate with each other using VLANs.

Mode Global Configuration Mode

Default dot1q-vlan (VLAN aware bridging)

Note: The VLAN mode can be configured, only if the VLAN switching feature is started and enabled in the switch.

Example

```
Your Product(config)# base bridge-mode dot1d-bridge
```

Related Command(s)

- `shutdown garp` - Shuts down the GARP module in the switch on all ports and releases all memories used for the GARP module..
- `shutdown snooping` - Shuts down snooping in the switch.
- `shutdown spanning-tree` - Shuts down spanning tree functionality in the switch.
- `spanning-tree mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `shutdown port-channel` - Shuts down LA in the switch and releases the allocated resources to the switch.
- `shutdown lldp` - Shuts down all the ports in the LLDP and releases all the allocated memory.
- `interface-configuration and deletion` - Allows to configure interface such as out of band management, port channel, tunnel, and so on.
- `set vlan` - Globally enables / disables VLAN feature in the switch (that is the status of the VLAN feature is configured for all ports of the switch).
- `vlan` - Creates a VLAN in the ISS and enters into the config -VLAN mode in which VLAN specific configurations are done.
- `mac-vlan` - Enables MAC-based VLAN membership classification on all ports of the switch.
- `subnet-vlan` - Enables subnet-VLAN based membership classification on all ports of the switch.
- `protocol-vlan` - Enables protocol-VLAN based membership classification on all ports of the switch
- `map protocol` - Creates a protocol group with a specific protocol and encapsulation frame type combination.
- `set gvrp` - Globally enables / disables GVRP feature on all ports of a switch.
- `set gmrp` - Globally enables / disables GMRP feature on all ports of a switch.
- `set vlan traffic-classes` - Enables or disables traffic class feature in a switch on all ports.
- `switchport filtering-utility-criteria` - Creates filtering utility criteria for the port.
- `mac-address-table static unicast` – Transparent Bridging Mode - Configures a static unicast MAC address in the forwarding database when base bridge mode is transparent bridging in order to control unicast packets to be processed.
- `mac-address-table static multicast` – Transparent Bridging mode- Configures a static multicast MAC address in the forwarding database in transparent bridging mode in order to control multicast packets to be processed.

- `wildcard` - Configures the wildcard VLAN entry for a specified MAC address or any MAC address.
- `set unicast-mac learning` - Enables or disables unicast-MAC learning feature for a VLAN.
- `vlan unicast-mac learning limit` - Configures the unicast-MAC learning limit for a VLAN.
- `unicast-mac learning limit` - Configures the unicast-MAC learning limit for a switch.
- `vlan active` - Activates a VLAN in the switch.
- `switchport pvid` - Configures the PVID on the specified port.
- `switchport acceptable-frame-type` - Configures the type of VLAN dependant BPDU frames such as GMRP BPDU, that the port should accept during the VLAN membership configuration.
- `switchport ingress-filter` - Enables ingress filtering feature on the port.
- `switchport map protocols-group` - Maps the protocol group configured to a particular VLAN identifier for the specified interface
- `switchport priority default` - Sets the default user priority for the port
- `switchport mode` - Configures the mode of operation for a switch port.
- `switchport map protocols-group` - Maps the configured protocol group to a particular VLAN ID for an interface.
- `switchport priority default` - Configures the default ingress user priority for a port.
- `switchport protected` - Enables switchport protection feature for a port.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan device info` - Displays the VLAN global information that is applicable to all VLANs created in the switch / all contexts.

mac-vlan

Command Objective This command enables MAC-based VLAN membership classification on all ports of the switch. VLAN membership classification is done based on the MAC address of the source of received packets. The VLAN membership should be assigned initially, if the MAC-based VLAN membership classification is to be enabled in the switch.

The no form of the command disables MAC-based VLAN membership classification on all ports of the switch.

Syntax **mac-vlan**

no mac-vlan

Mode Global Configuration Mode

Default MAC-based VLAN membership classification is disabled on all ports of the switch.

Note: MAC-based VLAN membership classification cannot be configured in the switch, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.

Example

```
Your Product(config)# mac-vlan
```

Related Command(s)

- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `mac-map` - Configures the VLAN-MAC address mapping that is used only for MAC-based VLAN membership classification.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan device info` - Displays the VLAN global information that is applicable to all VLANs created in the switch / all contexts.
- `show mac-vlan` - Displays all entries in the MAC map table.

subnet-vlan

Command Objective This command enables subnet-VLAN based membership classification on all ports of the switch. The source IP address in received packet is matched to a VLAN ID using an administrator configured table to perform VLAN membership classification.

The no form of the command disables subnet-VLAN based membership classification on all ports of the switch.

Syntax **subnet-vlan**

no subnet-vlan

Mode Global Configuration Mode

Default Subnet-based VLAN membership classification is disabled on all ports of the switch.

Note: Subnet-VLAN based membership classification cannot be configured in the switch, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.

Example

```
Your Product(config)# subnet-vlan
```

Related Command(s)

- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `map subnet` - Configures VLAN-IP subnet address mapping that is used only for subnet-VLAN based membership classification.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan device info` - Displays the VLAN global information that is applicable to all VLANs created in the switch / all contexts.
- `show subnet-vlan mapping` - Displays all entries in the subnet map table.

protocol-vlan

Command Objective This command enables protocol-VLAN based membership classification on all ports of the switch. VLAN membership classification is done for all untagged and priority-tagged frames based on the port-protocol group / higher layer protocol for the port.

The no form of the command disables protocol-VLAN based membership classification on all ports of the switch.

Syntax **protocol-vlan**

no protocol-vlan

Mode Global Configuration Mode

Default Protocol-based VLAN membership classification is enabled on all ports of the switch.

Note: Protocol-VLAN based membership classification cannot be configured in the switch, if the base bridge mode is set as transparent bridging or the VLAN switching feature is

Example

```
Your Product(config)# no protocol-vlan
```

Related Command(s)

- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `port protocol-vlan` - Enables protocol-VLAN based membership classification in a port.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan device info` - Displays the VLAN global information that is applicable to all VLANs created in the switch / all contexts

map protocol

Command Objective This command creates a protocol group with a specific protocol and encapsulation frame type combination.

The created protocol group is used for protocol-VLAN based membership classification. The specified protocol is applied above the data-link layer in a protocol template, and the frame type is applied in the template.

The no form of the command deletes all group that have the specified protocol and encapsulation frame type combination.

Syntax **map protocol {ip | novell | netbios | appletalk | other <aa:aa or aa:aa:aa:aa:aa>} {enet-v2 | snap | llcOther | snap8021H | snapOther} protocols-group <Group id integer(0-2147483647)>**

no map protocol {ip | novell | netbios | appletalk | other <aa:aa or aa:aa:aa:aa:aa>} {enet-v2 | snap | llcOther | snap8021H | snapOther}

Parameter Description

- `ip` - Sets the protocol as IP, which is used for communicating data across network using TCP / IP.

The corresponding octet string is 08:00.

- `novell` - Sets the protocol as Novell Netware protocol suite, which is developed by Novell Inc. The corresponding octet string is ff:ff.
- `netbios` - Sets the protocol as NetBIOS over TCP/IP, which allows legacy application relying on NetBIOS API to be used on modern TCP/IP networks. The corresponding octet string is f0:f0. This protocol can be set only for the encapsulation frame type llcOther.
- `appletalk` - Sets the protocol as AppleTalk, which is a proprietary suite of protocols developed by Apple Inc. The corresponding octet string is 80:9b.
- `other` - Sets the protocol type using its corresponding octet string. This value is used to configure some other protocol type other than ip, novell, netbios and appletalk and also the listed protocol types. This value is set as:
    - 16-bit (2 octet) IEEE 802.3 type field, if the frame type is set as enet-v2, snap and snap8021H.
    - 40-bit (5 octet) PID, if the frame type is set as snapOther.
    - 2 octet IEEE 802.2 LSAP pair, if the frame type is set as llcother. The first octet is used for DSAP and the second octet is used for SSAP.
- `enet-v2` - Applies the standard IEEE 802.3 frame format. This format contains:
    - `Preamble` – 7 byte value that allows the Ethernet card to synchronize with the beginning of a frame.
    - `SFD`– 1 byte value that indicates the start of a frame.
    - `Destination`– 6 byte MAC address of the destination.
    - `Source` – 6 byte MAC address of the source or a broadcast.
    - `Length` – 2 byte value representing the number of bytes in the data fields.
    - `Data` – 46 to 1500 bytes higher layer information containing protocol information or user data.
    - `FCS` – 4 byte value representing the cyclic redundancy check used by source and destination to verify a successful transmission.
- `snap` - Applies the sub-network access protocol format. This format contains the same structure as LLC format except the following additional fields added before the data field:
    - `OUI` – 3 byte value representing organizational unique ID assigned to vendors for differentiating protocols from different manufacturers.
    - `Type` – 2-byte value representing protocol type that defines a specific protocol in the SNAP. This maintains compatibility with Ethernet v2.
- `llcOther` - Applies the LLC format. This format contains the same structure as IEEE 802.3 frame except the following additional fields added before the data field:
    - `DSAP` – 1 byte value representing destination service access point to determine the protocol used for the upper layer.
    - `SSAP` – 1 byte value representing source service access point to determine the protocol used for the upper layer.

    - `Control` **–** 1 byte value that is used by certain protocols for administration.
- `snap8021H` - Applies the sub-network access protocol format. This format contains the same structure as LLC format except for two additional fields before the data field as mentioned below:
    - `3 octet` - field having value 00:00:F8 signifying that next 2 octet field is the encoding of 802.3 Type field in an IEEE 802.2/SNAP Header.
    - `2 octet Type field` - encoding of 802.3 Type field in an IEEE 802.2/SNAP Header
- `snapOther` - Applies the sub-network access protocol format. This format contains the same structure as LLC format except for an additional 5 octet SNAP Protocol Identifier (PID) added before the data field. The value of the PID is not in ether of the ranges used for RFC_1042(SNAP) or SNAP 802.1H. This frame type can be set only for some other protocol type other than ip, novell, netbios and appletalk.
- `<Group id integer(0-2147483647)>` - Configures a unique group ID that is to be created with the specified protocol type and encapsulation frame type. This value represents a specific group of protocols that are associated together when assigning a VID to a frame. This value ranges between 0 and 2147483647.

Mode Global Configuration Mode

Note: Protocol group cannot be created and configured in the switch, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.

Example

```
Your Product(config)# map protocol ip enet-v2 protocols- group 1
```

Related Command(s)

- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `switchport map protocols-group` - Maps the configured protocol group to a particular VLAN ID for an interface.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan protocols-group` - Displays all entries in the protocol group table.

set vlan traffic-classes

Command Objective This command enables or disables traffic class feature in a switch on all ports.

Traffic class feature is used to meet the latency and throughput requirement of time-critical traffic in a LAN environment, where both time-critical and non-time- critical traffic compete for the network bandwidth.

Syntax **set vlan traffic-classes {enable | disable}**

Parameter Description

- `enable` - Enables traffic class feature in the switch on all ports. You can assign user priority to the particular traffic class.

- `disable` - Disables traffic class feature in the switch on all ports. The switch operates with a single priority level for all traffics

Mode Global Configuration Mode

Default enable

Note: The traffic class feature cannot be configured in the switch, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.

Example

```
Your Product(config)# set vlan traffic-classes disable
```

Related Command(s)

- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan device info` - Displays the VLAN global information that is applicable to all VLANs created in the switch / all contexts.

mac-address-table static unicast

Command Objective This command configures a static unicast MAC address in the forwarding database.

The no form of the command deletes a configured static Unicast MAC address from the forwarding database.

Syntax **mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id/vfi_id> [{recv-port <ifXtype> <ifnum> }] [interface ([<interface-type> <0/a-b, 0/c, ...>] [<interface-type> <0/a-b, 0/c, ...>] [port-channel <a,b,c- d>][pw <a,b,c-d>][ac <a,b, c-d>])] [connection-identifier <ucast_mac>] [status { permanent | deleteOnReset |deleteOnTimeout }]**

no mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id/vfi_id> [{recv-port <ifXtype> <ifnum>}]

Parameter Description

- `<aa:aa:aa:aa:aa:aa>` - Configures the static unicast destination MAC address. The received packets having the specified MAC address are processed.
- `vlan <vlan-id/vfi-id>` - Configures the static unicast destination MAC address for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - `<vlan –id>` - VLAN ID is a unique value that represents the specific - VLAN. This value ranges between 1 and 4094
  - `<vfi-id>`. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This feature is not supported.
    - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.

        - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
        - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- `recv-port` - Configures the receive ports details. The static unicast packets received only on this specified port are processed. The details to be provided are:
    - `<interface-type>` - Configures the receive ports details for the specified type of interface. The interface can be:
        - `qx-ethernet` –A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
        - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
        - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
        - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
    - `<interface-id>` - Configures the receive ports details for the specified type of interface. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel.
- `interface` - Configures the member ports interface type and ID. The details to be provided are:
    - `<interface-type>` - Configures the member ports for the specified type of interface. The interface can be:
        - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
        - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
        - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
        - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
    - `<0/a-b, 0/c, ...>` - Configures the member ports for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel.
- `port-channel<a,b,c-d>` - Sets the list of port channel interfaces or a specific port channel

identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.

- `pw <a,b,c-d>` - Configures a static unicast MAC address for the specified pseudowire interface. When the pseudo wire interface is mapped to a specific VLAN, interface structures are created. This value ranges between 1 and 65535.Use comma as a separator without space while configuring list of interfaces. Example: 1,3.. This interface type is not supported.
- `ac <a,b, c-d>` - Configures a static unicast MAC address for the specified attachment circuit interface. This value ranges between 1 and 65535. Use comma as a separator without space while configuring list of interfaces. Example: 1,3. This interface type is not supported.
- `connection-identifier<ucast_mac>` - Associates backbone MAC address of peer backbone edge bridge with customer MAC address that can be reached through the bridge.
- `status` - Specifies the status of the Static unicast entry. The options are:
  - permanent - Entry remains even after the next reset of the bridge
  - deleteOnReset - Entry remains until the next reset of the bridge
  - deleteOnTimeout - Entry remains until it is aged out

Mode Global Configuration Mode

Default status - permanent

Notes:

- VLAN/Service-instance must have been configured and member ports must have been configured for the specified VLAN/Service-instance.
- The VLAN value in a configured static MAC entry must be active
- The new configured ports are appended to the existing member port list of the vlan
- The Egress port value and receive port value in a configured static MAC entry must be a member of the configured VLAN. Receive Port cannot be an Egress port in a configured static MAC entry

Example

```
Your Product(config)# mac-address-table static unicast 00:11:22:33:22:11 vlan 3 recv-
port gigabitethernet 0/2 interface gigabitethernet 0/1 status deleteOnTimeout
Your Product(config)# mac-address-table static unicast 00:11:22:33:22:11 vlan 1 recv-
port gigabitethernet 0/2 interface gigabitethernet 0/1 pw 1
Your Product(config)# mac-address-table static unicast 00:11:22:33:22:11 vlan 4099 recv-
port gigabitethernet 0/2 interface ac 1
```

Related Command(s)

- `mac-address-table static multicast` - Configures a static multicast MAC address in the forwarding database.
- `vlan` - Configures a VLAN in the switch and enters the config-VLAN mode.
- `ports` - Statically configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN.
- `vlan active` - Activates a VLAN in the switch.
- `show mac-address-table static unicast` - Displays the statically configured unicast address

from the MAC address table.

mac-address-table static unicast – Transparent Bridging Mode

Command Objective This command configures a static unicast MAC address in the forwarding database in transparent bridging mode in order to control unicast packets to be processed. Only the unicast packets having the configured value are processed.

The no form of the command deletes the configured static unicast address from the forwarding database.

Syntax **mac-address-table static unicast <aa:aa:aa:aa:aa:aa> [recv- port <interface-type> <interface-id>] interface ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>]) [status { permanent | deleteOnReset | deleteOnTimeout }]**

no mac-address-table static unicast <aa:aa:aa:aa:aa:aa> [recv-port <interface-type> <interface-id>]

Parameter Description

- `<aa:aa:aa:aa:aa:aa>` - Configures the unicast destination MAC address. The received packets having the specified MAC address are processed.
- `recv-port` - Configures the receive port's details. The unicast packets received only on this specified port are processed. The details to be provided are:
  - `<interface-type>` - Sets the type of interface. The interface can be:
  - `qx-ethernet` –A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
  - `<interface-id>` - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel.
- `interface` - Configures the member ports details. The unicast packets received on the specified receive ports and having the specified unicast destination MAC address are forwarded through these member ports. The details to be provided are:
  - `<interface-type>` - Sets the type of interface. The interface can be:

        - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
        - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
        - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
        - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
    - `<0/a-b, 0/c, ...>` - Sets the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel. Use comma as a separator withoutspace while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
- `port-channel<a,b,c-d>` - Sets the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
- `status` - Configures the status of the static unicast entry. The options are:
    - `permanent` - The static unicast entry resides in the switch, even after restarting the switch.
    - `deleteOnReset` - The static unicast entry is deleted, once the switch is restart.
    - `deleteOnTimeout` - The static unicast entry is deleted once the MAC address table aging timer expires.

Mode Global Configuration Mode

Default status - permanent

Notes:

- This command is applicable only if the base bridge mode is set as transparent bridging.
- The interface gigabitethernet 0/1 cannot be set as member port or receive port in the static entry, as it is configured as a router port in transparent bridging mode.
- The same interface cannot be configured as both ingress port (receive port) and egress port (member port). The port can act only as ingress or as egress.
- If the receive port is configured in the created static unicast MAC address entry, then that entry can be deleted only if the receive port details are exactly mentioned in the no form of the command.
- Only one static unicast MAC address entry is allowed in the switch in transparent bridging mode. If any updates need to be done in the existing one, then it should be deleted and new entry should be created with new configurations.

Example

```
Your Product(config)# mac-address-table static unicast 00:11:22:33:44:55
recv-port gigabitethernet 0/3 interface gigabitethernet 0/2 status
deleteOnTimeout
```

Related Command(s)

- `base bridge-mode dot1d-bridge` - Configures the VLAN operation mode as transparent bridging.
- `mac-address-table aging-time` - Configures the timeout period (in seconds) for aging out dynamically learned forwarding information entry and static entry in the MAC address table.
- `show dot1d mac-address-table` - Displays all static / dynamic unicast and multicast MAC address entries created in the FDB table, when the VLAN base bridge mode is transparent bridging.
- `show dot1d mac-address-table static unicast`- Displays all static unicast MAC address entries created in the FDB table, when the VLAN base bridge mode is transparent bridging.

mac-address-table static multicast

Command Objective This command configures a static multicast MAC address in the forwarding database.

Syntax **mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id/vfi_id> [recv-port <ifXtype> <ifnum>] interface ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>][pw <a,b,c-d>] [ac <a,b,c-d>]) [forbidden-ports ([<interface-type> <0/a- b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port- channel <a,b,c-d>][pw <a,b,c-d>][ac <a,b,c-d>])] [status { permanent | deleteOnReset | deleteOnTimeout }]**

no mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id/vfi_id> [recv-port <ifXtype> <ifnum>}]

Parameter Description

- `<aa:aa:aa:aa:aa:aa>` - Configures the multicast destination MAC address. The received packets having the specified MAC address are processed.
- `vlan <vlan-id/vfi-id>` - Configures the static multicast destination MAC address for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - `<vfi-id>.` - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This feature is not supported.

  Notes:

  1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
  2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
  3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs

are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- `recv-port` - Configures the receive port's details. The multicast packets received only on this specified port are processed. The details to be provided are:
  - `<ifXtype>` - Sets the type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
  - `<ifnum>` - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID isprovided, for interface types port-channel.
- `interface` - Configures the member ports details. The multicast packets received on the specified receive ports and having the specified multicast destination MAC address are forwarded through these member ports. The details to be provided are:
  - <interface-type> - Sets the type of interface. The interface can be:
    - qx-ethernet – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
  - `<0/a-b, 0/c, ...>` - Sets the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel. Use comma as a separator withoutspace while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
  - `port-channel <a,b,c-d>` - Sets the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
  - `pw <a,b,c-d>` - Configures a static multicast MAC address the Pseudo wire interface. When

the pseudo wire interface is mapped to a specific VLAN, the interface structures are created. This value ranges between 1 and 65535. This interface type is not supported.

Note: Maximum number of PseudoWire interfaces supported in the system is 100.

- ac <a,b, c-d> - Configures a static multicast MAC address for the specified attachment circuit interface. This value ranges between 1 and 65535. Use comma as a separator without space while configuring list of interfaces. Example: 1,3. This interface type is not supported.

- forbidden-ports - Configures the ports for which GMRP should not dynamically register the service requirement attribute forward all multicast groups. This configuration is restored once the switch is reset. The details to be provided are:
  - <interface-type> - Sets the type of interface. The interface can be:
    - qx-ethernet – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - gigabitethernet - A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - extreme-ethernet - A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - port-channel - Logical interface that represents an aggregator which contains several ports aggregated together.
  - <0/a-b, 0/c, ...> - Sets the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel. Use comma as a separator withoutspace while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
  - port-channel <a,b,c-d> - Sets the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3
  - pw <a,b,c-d> - Configures the Pseudo wire interface. When the pseudo wire interface is mapped to a specific VLAN, the interface structures are created. This value ranges between 1 and 65535. This interface type is not supported.

    Note: Maximum number of PseudoWire interfaces supported in the system is 100

  - ac <a,b, c-d> - Configures a static multicast MAC address for the specified attachment circuit interface. This value ranges between 1 and 65535. Use comma as a separator without space while configuring list of interfaces. Example: 1,3. This interface is not supported.
- status - Status of the static multicast entry. The options are:
  - permanent - Entry remains even after the next reset of the bridge
  - deleteOnReset - Entry remains until the next reset of the bridge
  - deleteOnTimeout - Entry remains until it is aged out

Mode Global Configuration Mode

Default status - permanent

Notes:

- VLAN/Service-instance must have been configured and member ports must have been configured for the specified VLAN/Service-instance.
- The VLAN value in a configured static MAC entry must be active
- The new configured ports are appended to the existing member port list of the VLAN
- The Egress Port value and Receive Port value in a configured static MAC entry must be a member of the configured VLAN
- Receive Port cannot be an Egress port in a configured static MAC entry

Example

```
Your Product(config)# mac-address-table static multicast
01:02:03:04:05:06 vlan 2 interface gigabitethernet 0/1
```

Related Command(s)

- `mac-address-table static unicast` - Configures a static unicast MAC address in the forwarding database.
- `vlan` - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode.
- `ports` - Statically configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN. The VLAN can also be activated using the vlan active command.
- `vlan active` - Activates a VLAN in the switch.
- `show mac-address-table static multicast` - Displays the statically configured multicast entries.

mac address-table static mcast

Command Objective This command configures a static multicast MAC (Media Access Control) address in the forwarding database.

The no form of the command deletes a configured static multicast MAC address from the forwarding database.

Notes:

1. This command is a complete standardized implementation of the existing command and operates similar to that of the command mac-address-table static multicast.
2. This feature has been included in adherence to the Industry Standard CLI syntax.

Syntax **mac address-table static <mcast_mac> vlan <integer(1-4094)> ([interface <interface-type> <0/a-b,0/c,...>] [<interface- type> <0/a-b,0/c,...>][port-channel <a,b,c-d>])**

no mac address-table static <mcast_mac> vlan <vlan-id(1-4094)> [interface <ifXtype>

<ifnum>]

Parameter Description

- `<mcast_mac>` - Configures the static MAC address that should be mapped to the specified VLAN and used for MAC based VLAN membership classification.
- `vlan<integer(1-4094)>` - Configures the VLAN ID to which the configured MAC address should be mapped. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
- `interface` - Configures the member ports details. The static packets received on the specified receive ports and having the specified static destination MAC address are forwarded through these member ports. The details to be provided are:
  - <interface-type> - Sets the type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `internal-lan` – Internal LAN created on a bridge per IEEE 802.1ap.
    - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<0/a-b, 0/c, ...>` - Sets the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
  - port-channel<a,b,c-d> - Sets the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.

Mode Global Configuration Mode

Note:

- VLAN must have been configured and member ports musthave been configured for the specified VLAN.
- The VLAN value in a configured static MAC entry must be active

Example

```
Your Product(config)# mac address-table static

01:02:03:04:05:06 vlan 2 interface gigabitethernet 0/1
```

Related Command(s)

- show mac-address-table static multicast - Displays the statically configured multicast entries.
- vlan - Configures a VLAN in the switch and is also used to enter in to the config-VLAN mode.
- vlan active - Activates a VLAN in the switch.
- ports - Configures a VLAN entry.

mac-address-table static multicast – Transparent Bridging mode

Command Objective This command configures a static multicast MAC address in the forwarding database in transparent bridging mode in order to control multicast packets to be processed. Only the multicast packets having the configured value are processed.

This configuration is used to filter incoming reports that can be commonly used by all multicast protocols.

The no form of command deletes the configured static multicast MAC address from the forwarding database.

Syntax **mac-address-table static multicast <aa:aa:aa:aa:aa:aa> [recv-port <interface-type> <interface-id>] interface ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>]]) [status { permanent | deleteOnReset | deleteOnTimeout }]**

no mac-address-table static multicast <aa:aa:aa:aa:aa:aa> [recv-port <interface-type> <interface-id>]

Parameter Description

- <aa:aa:aa:aa:aa:aa> - Configures the multicast destination MAC address. The received packets having the specified MAC address are processed.
- recv-port - Configures the receive port's details. The multicast packets received only on this specified port are processed. The details to be provided are:
    - <ifXtype> - Sets the type of interface. The interface can be:
        - qx-ethernet – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
        - gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
        - extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
        - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
    - <ifnum> - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash,

for interface type other than port-channel. Only port-channel ID isprovided, for interface type port-channel.

- `interface` - Configures the member ports details. The multicast packets received on the specified receive ports and having the specified multicast destination MAC address are forwarded through these member ports. The details to be provided are:
  - `<interface-type>` - Sets the type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
  - `<0/a-b, 0/c, ...>` - Sets the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel. Use comma as a separator withoutspace while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
  - `port-channel <a,b,c-d>` - Sets the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
- `status` - Configures the status of the static multicast entry. The options are:
  - `permanent` - The static multicast entry resides in the switch, even after restarting the switch.
  - `deleteOnRese`t - The static multicast entry is deleted, once the switch is restart.
  - `deleteOnTimeout` - The static multicast entry is deleted once the MAC address table aging timer expires.

Mode Global Configuration Mode

Default status - permanent

Notes:

- This command is applicable only if the base bridge mode is set as transparent bridging.
- The interface gigabitethernet 0/1 cannot be set as member port or receive port in the static entry, as it is configured as a router port in transparent bridging mode.
- The same interface cannot be configured as both ingress port (receive port) and egress port (member port). The port can act only as ingress or as egress.
- If the receive port is configured in the created static multicast MAC address entry, then that entry can be deleted only if the receive port details are exactly mentioned in the no form of the command.

- Only one static multicast MAC address entry is allowed in the switch in transparent bridging mode. If any updates need to be done in the existing one, then it should be deleted and new entry should be created with new configurations.

Example

```
Your Product(config)# mac-address-table static multicast
01:00:5E:01:02:03interface gigabitethernet 0/2
```

Related Command(s)

- `base bridge-mode dot1d-bridge` - Configures the VLAN operation mode as transparent bridging.
- `mac-address-table aging-time` - Configures the timeout period (in seconds) for aging out dynamically learned forwarding information entry and static entry in the MAC address table.
- `show dot1d mac-address-table` - Displays all static / dynamic unicast and multicast MAC address entries created in the FDB table, when the VLAN base bridge mode is transparent bridging.
- `show dot1d mac-address-table static multicast` - Displays all static multicast MAC address entries created in the FDB table, when the VLAN base bridge mode is transparent bridging.

mac-address-table aging-time

Command Objective This command configures the timeout period (in seconds) for aging out dynamically learned forwarding information entry and static entry in the MAC address table. That is, the entry is deleted once the aging timer expires. High value for the aging time helps to record dynamic entries for a longer time, if traffic is not frequent. This reduces the possibility of flooding.

The no form of the command resets the maximum age of an entry in the MAC address table to its default value.

Syntax **mac-address-table aging-time <10-1000000 seconds>**

no mac-address-table aging-time

Mode Global Configuration Mode

Default 300

Notes:

- The aging timer is applied to the static entry in the MAC address table, only if static entry status is set as deleteOnTimeout.
- The MAC address table maximum age can be configured in the switch, only if the VLAN switching feature is started and enabled in the switch.

Example

```
Your Product(config)# mac-address-table aging-time 200
```

Related Command(s)

- `mac-address-table static unicast` – Transparent Bridging Mode - Configures a static unicast MAC address in the forwarding database in transparent bridging mode in order to control unicast packets to be processed.
- `mac-address-table static multicast` – Transparent Bridging mode - Configures a static multicast MAC address in the forwarding database in transparent bridging mode in order to control multicast packets to be processed.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show mac-address-table aging-time` - Displays the ageing time configured for the MAC address table.

clear vlan statistics

Command Objective This command clears VLAN counters that maintain statistics information on a per VLAN basis.

The counter is cleared for all available VLANs or for the specified VLAN. The statistics information contains number of unicast, broadcast and unknown unicast packets flooded.

Syntax **clear vlan statistics [vlan <vlan-id/vfi_id>]**

Parameter Description

- `vlan <vlan-id/vfi-id>` - Clears VLAN counters for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This is not supported.

  Notes:

  - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
  - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
  - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

Mode Global Configuration Mode

Note: The information is the VLAN counters can be deleted, only if the VLAN switching feature is started and enabled in the switch.

Example `Your Product(config)# clear vlan statistics vlan 1`

Related Command (s)

- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan statistics` - Displays the unicast / broadcast statistics details of all active VLANs and VLANs (that are not active) for which the port details are configured.

wildcard

Command Objective This command configures the wildcard VLAN entry for a specified MAC address or any MAC address.

The wild card VLAN static filtering information is used for all VLANs for which no static unicast and multicast MAC address entries are created.

The no form of the command deletes the wildcard entry for the specified MAC address or broadcast address.

Syntax **wildcard {mac-adddress <mac_addr> | broadcast} interface ([<interface-type> <0/a-b, 0/c, ...>] [<interface-type> <0/a-b, 0/c, ...>] [port-channel <a,b,c-d>][pw <a,b,c-d>] [ac <a,b,c-d>]))**

no wildcard {mac-adddress <mac_addr> | broadcast}

Parameter Description

- `mac-adddress<mac_addr>` - Configures the destination unicast or multicast MAC address to which filtering information of wild card entry should be applied. The received frames that contain the configured MAC address are forwarded through the specified interface, if no specific static filtering is configured for that MAC address.
- `broadcast` - Configures automatically the destination MAC address as ff:ff:ff:ff:ff:ff. The received frames that contain any MAC address are forwarded through the specified interface, if no specific filtering is configured for that MAC address.
- `interface` - Configures the member ports details. The received frames having the specified destination MAC address are forwarded through these member ports. The details to be provided are:
  - `<interface-type>` - Sets the type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.

        - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
    - `<0/a-b, 0/c, ...>` - Sets the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel. Use comma as a separator withoutspace while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
- `port-channel <a,b,c-d>` - Sets the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
- `pw <a,b,c-d>` - Sets Pseudo wire interface. When the pseudo wire interface is mapped to a specific VLAN, the interface structures are created. This value ranges between 1 and 65535. This interface type is not supported.

  Note: Maximum number of PseudoWire interfaces supported in the system is 100.

- `ac <a,b, c-d>` - Configures the wildcard entry for the specified ac identifier or a list of identifiers. This value ranges between 1 and 65535. Use comma as a separator without space while configuring list of interfaces. Example: 1,3. This interface type is not supported.

Mode Global Configuration Mode

Notes:

- The wildcard VLAN entry cannot be configured in the switch, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.
- This command executes only if statically a VLAN entry is configured with the required member ports

Example

```
Your Product(config)# wildcard mac-address
01:02:03:04:05:06 interface gigabitethernet 0/1
```

Related Command(s)

- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show wildcard` - Displays all wildcard MAC entries created in the switch / in all contexts.
- `ports` - Statically configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN. The VLAN can also be activated using the vlan active command.

unicast-mac learning limit

Command Objective This command configures the unicast-MAC learning limit for a switch. The limit represents the maximum number of distinct unicast MAC addresses that can be learnt in the switch. This value ranges between 0 and 4294967295.

The maximum number of unicast MAC addresses learnt differs for SMIS models. Some models may not support because of hardware limitation.

The no form of the command resets the unicast-MAC learning limit for the switch to its default value.

Syntax **unicast-mac learning limit <limit value(0-4294967295)>**

no unicast-mac learning limit

Mode Global Configuration mode

Default The maximum limit supported by the switch.

Notes:

- The limiting value should not be less than the unicast MAC learning limit set for any of the VLAN.
- Unicast-MAC learning limit cannot be configured in the switch, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.

Example Your Product(config)# unicast-mac learning limit 5

Related Command(s)

- `base bridge-mode dot1q-vlan` – Configures the VLAN operation mode as VLAN aware bridging.
- `vlan unicast-mac learning limit` - Configures the unicast-MAC learning limit for a VLAN.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan device info` - Displays the VLAN global information applicable to all VLANs created in the switch / all contexts.

map subnet

Command Objective This command configures VLAN-IP subnet address mapping that is used only for subnet-VLAN based membership classification.

In subnet-VLAN based membership classification, the source IP address in received packet is matched to a VLAN ID using this mapping entry to perform VLAN membership classification.

The no form of the command deletes the VLAN-IP subnet address mapping entry.

Syntax **map subnet <ip-subnet-address> vlan <vlan-id/vfi_id> [arp {suppress | allow}][mask <subnet-mask>]**

no map subnet <ip-subnet-address> [mask <subnet-mask>]

Parameter Description

- `<ip-subnet-address>` - Configures the IP subnet address to be used for deciding on discarding / allowing of ARP frames.
- `vlan <vlan-id/vfi-id>` - Configures VLAN-IP subnet address mapping for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
    - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
    - `<vfi-id>` - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

      Notes:

        - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
        - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
        - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- `arp` - Configures the way of handling of ARP untagged frames on the specified VLAN. The options are:
    - `suppress` - Does not perform VLAN classification for ARP frames having the specified source IP subnet address.
    - `allow` - Performs VLAN classification for ARP frames having the specified source IP subnet address.

      Note: This parameter is not supported in some SMIS models. The ARP option cannot be configured as allow, when the hardware does not classify ARP broadcast packets based on subnet VLAN mapping. In such case, subnet VLAN mapping works only on IP packets.
- `mask <subnet-mask>` - Configures the subnet mask address to be used for deciding on discarding / allowing of ARP frames.

Mode Global Configuration Mode

Default arp - Suppress for all boa, rds

Notes:

- Only the VLANs that are activated in the switch can be mapped to the specified IP subnet address.
- VLAN-IP subnet address mapping can be configured in the port, only if the VLAN

switching feature is started and enabled in the switch.

Example

```
Your Product(config-if)# map subnet 14.0.0.0 vlan 1 arp allow
```

Related Command(s)

- `subnet-vlan` - Enables subnet-VLAN based membership classification on all ports of the switch.
- `vlan active` - Activates a VLAN in the switch.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show subnet-vlan mapping` - Displays all entries in the subnet map table.

ports

Command Objective This command statically configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN. The VLAN can also be activated using the vlan active command.

The configuration defines the tagged and untagged member ports that are used for egress tagging of a VLAN at a port.

The no form of the command deletes the specified port details for the VLAN. The member ports cannot be set empty for the VLAN, once the member ports details are configured for that VLAN.

Syntax **ports [add] ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>][pw <a,b,c-d>]) [untagged <interface-type> <0/a-b,0/c,...> [<interface-type> <0/a-b,0/c,...>] [port- channel <a,b,c-d>] [pw <a,b,c-d>] [ac <a,b,c-d>] [all])] [forbidden <interface-type> <0/a-b,0/c,...> [<interface- type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c- d>] [ac <a,b,c-d>]] [name <vlan-name>]**

no ports [<interface-type> <0/a-b,0/c,...>] [<interface- type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c- d>] [ac <a,b,c-d>] [all] [untagged ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port- channel <a,b,c-d>] [pw <a,b,c-d>] [ac <a,b,c-d>] [all])] [forbidden ([<interface-type> <0/a-b,0/c,...>] [<interface- type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c- d>] [ac <a,b,c-d>] [all])] [name <vlan-name>]

Parameter Description

- `add` - Appends the new configured ports to the existing member port list of the vlan
- `<interface-type> <0/a-b,0/c,...>` - Configures the ports that should be set as a member of the VLAN. The details to be provided are:
  - `<interface-type>` - Sets the type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data

transfer up to 1 Gigabit per second.

        - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
        - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
    - `<0/a-b, 0/c, ...>` - Sets the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel. Use comma as a separator withoutspace while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
- `port-channel<a,b,c-d>` - Sets the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
- `pw <a,b,c-d>` - Configures the Pseudo wire interface as member port. When the pseudo wire interface is mapped to a specific VLAN, the interface structures are created. This value ranges between 1 and 65535. This interface type is not supported.

  Note: Maximum number of PseudoWire interfaces supported in the system is 100.
- `ac <a,b, c-d>` - Configures the specified attachment circuit interface as a member port. This value ranges between 1 and 65535. Use comma as a separator without space while configuring list of interfaces. Example: 1,3. This interface type is not supported.
- `all` - Deletes all configured member ports for the VLAN and sets the member ports as none. This option is available only in the no form of the command.
- `untagged<interface-type> <0/a-b,0/c,...>` - Configures the ports that should be used for the VLAN to transmit egress packets as untagged packets. The details to be provided are:
    - `<interface-type>` - Sets the type of interface. The interface can be:
        - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
        - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
        - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
        - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
    - `<0/a-b, 0/c, ...>` - Sets the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
    - `port-channel` - Sets the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
    - `pw <a,b,c-d>` - Sets Pseudo wire interface. When the pseudo wire interface is mapped to

a specific VLAN, the interface structures are created. This value ranges between 1 and 65535. This interface type is not supported.

Note: Maximum number of PseudoWire interfaces supported in the system is 100.

- ac <a,b, c-d> - Configures the ac identifier or a list of identifiers to be used for the VLAN to transmit egress packets as untagged packets. This value ranges between 1 and 65535. Use comma as a separator without space while configuring list of interfaces. Example: 1,3. This interface type is not supported.
- all - Sets all configured member ports as the untagged ports for the VLAN.

Notes:

1. The ports configured should be a subset of the member ports.
2. The ports that are attached to VLAN-aware devices should always be set as untagged ports only.
3. The ports can be set as untagged ports, only if they are not configured as trunk ports.

- forbidden<interface-type> <0/a-b,0/c,...> - Configures the ports that should never receive packets from the VLAN. These ports drops the packets received from this VLAN. The details to be provided are:
  - <interface-type> - Sets the type of interface. The interface can be:
    - qx-ethernet – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
  - <0/a-b, 0/c, ...> - Sets the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1,3.
  - port-channel - Sets the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.
  - pw <a,b,c-d> - Sets the Pseudo wire interface as a port that should never receive packets from the VLAN. When the pseudo wire interface is mapped to a specific VLAN, the interface structures are created. This value ranges between 1 and 65535. This interface type is not supported

Note: Maximum number of PseudoWire interfaces supported in the system is 100.

- `ac <a,b, c-d>` - Sets the AC interface as a port that should never receive packets from the VLAN. This value ranges between 1 and 65535. Use comma as a separator without space while configuring list of interfaces. Example: 1,3. This interface type is not supported.
- `all` - Deletes all configured forbidden ports for the VLAN and sets the forbidden port as none. This option is available only in the no form of the command.

  The ports configured should not be a subset of the member ports. That is, the forbidden ports and member ports are mutually exclusive.

- `name<vlan-name>` - Configures the unique name of the VLAN. This name is used to identify the VLAN and is an administratively assigned string with the maximum size as 32.

Mode Config-VLAN Mode

Default All ports available in the switch are configured as member ports and untagged ports of the default VLAN (VLAN 1). For other active VLANs, the member, untagged and forbidden ports are not set (that is, set as none).

Example

```
Your Product(config-vlan)# ports gigabitethernet 0/1 pw 1 untagged
gigabitethernet 0/1 forbidden gigabitethernet 0/2 pw 2 name vl1

Your Product(config-vlan)# ports add gigabitethernet 0/1 ac 1 untagged
gigabitethernet 0/1 forbidden gigabitethernet 0/2 ac 2 name vl1
```

Related Command (s)

- `vlan active` - Activates a VLAN in the switch.
- `ports` - Statically configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN. The VLAN can also be activated using the vlan active command.
- `switchport mode` - Configures the mode of operation for a switch port.
- `show vlan` - Displays VLAN entry related information of all active VLANs and VLANs (that are not active) for which the port details are configured.
- `show vlan statistics` - Displays the unicast / broadcast statistics details of all active VLANs and VLANs (that are not active) for which the port details are configured.
- `show mac-address-table count` - Displays the total number of static / dynamic unicast and multicast MAC address entries created in the FDB table.
- `show vlan learning params` - Displays the VLAN learning parameter details for all active VLANs and VLANs (that are not active) for which the port details are configured, available in all contexts / in the switch.
- `set vlan counter` - Enables or disables the statistics collection for the specified VLAN.

vlan active

Command Objective This command activates a VLAN in the switch. The created VLANs should be active for further VLAN related configurations. The VLAN can also be activated using ports command.

Syntax **vlan active**

Mode Config-VLAN Mode

Default Only default VLAN (VLAN 1) is activated once the switch is started.

Note: VLAN cannot be made active, if base bridge mode is set as transparent bridging.

Example

```
Your Product(config-vlan)# vlan active
```

Related Command(s)

- `ports` - Statically configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN.
- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `mac-map` - Configures the VLAN-MAC address mapping that is used only for MAC-based VLAN membership classification.
- `map subnet` - Configures VLAN-IP subnet address mapping that is used only for subnet-VLAN based membership classification.
- `set unicast-mac learning` - Enables/ disables unicast-MAC learning feature for a VLAN.
- `vlan unicast-mac learning limit` - Configures the unicast-MAC learning limit for a VLAN.
- `switchport pvid` - Configures the PVID on the specified port.
- `show vlan` - Displays VLAN entry related information of all VLANs for which the port details are configured.
- `show vlan statistics` - Displays the unicast / broadcast statistics details of all VLANs for which the port details are configured.
- `show mac-address-table count` - Displays the total number of static / dynamic unicast and multicast MAC address entries created in the FDB table.
- `show vlan learning params` - Displays the VLAN learning parameter details for all VLANs for which the port details are configured, available in all contexts / in the switch.
- `set vlan counter` - Enables or disables the statistics collection for the specified VLAN.

set unicast-mac learning

Command Objective This command enables or disables unicast-MAC learning feature for a VLAN.

The source MAC learning is not done in the switch when this feature is disabled for the VLAN.

Syntax **set unicast-mac learning { enable | disable | default}**

Parameter Description

- `enable` - Enables unicast-MAC learning feature for a VLAN.
- `disable` - Disables unicast-MAC learning feature for a VLAN.
- `default` - Sets the unicast-MAC learning feature of the VLAN to its default state.

Mode Config-VLAN Mode

Default disable

Note:

- VLAN unicast-MAC learning feature cannot be configured in the VLAN, if the base bridge mode is set as transparent bridging.
- VLAN unicast-MAC learning feature can be configured only in the VLANs that are activated.

Example

```
Your Product(config-vlan)# set unicast-mac learning disable
```

Related Command(s)

- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `vlan active` - Activates a VLAN in the switch.
- `show vlan learning params` - Displays the VLAN learning parameter details for all active VLANs and VLANs (that are not active) for which the port details are configured, available in all contexts / in the switch.

interface range

Command Objective This command selects the range of physical interfaces and VLAN interfaces to be configured.

The no form of the command selects the range of VLAN interfaces to be removed.

Notes:

- This command is a complete standardized implementation of the existing command.
- This feature has been included in adherence to the Industry Standard CLI syntax.

Syntax **interface range ({ <interface-type> <slot/port-port>} {vlan <vlan-id(1-4094)> - <vlan-id(2-4094)>})**

no interface range vlan <vlan-id(1-4094)> - <vlan-id(2-4094)>

Parameter Description

- <interface-type> - Selects the range of the specified interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.

  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- <slot/port-port> - Selects the range of the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel.
- vlan <vlan-id(1-4094)> - <vlan-id(2-4094)> - Selects the range of the specified VLAN ID. This is a unique value that represents the specific VLAN created and activated. This value ranges between 1 and 4094.

  For specifying the interface VLAN range, space should be provided before and after the dash. That is, the command interface range vlan 1 – 4 is valid, whereas the command interface range vlan 1–4 is not valid.

Mode Global Configuration Mode

Note: For port channel range, the specified range must be configured using the interface command.

Example

```
Your Product(config)# interface range gigabitethernet 0/1 vlan 1 - 2
Your Product(config-if-range)#
Your Product(config)# interface range vlan 1 - 4 gigabitethernet 0/1
Your Product(config-if-range)#
```

Related Command(s)

- interface – Enters into the interface mode.
- show interfaces description - Displays the interface status and configuration.

vlan unicast-mac learning limit

Command Objective This command configures the unicast-MAC learning limit for a VLAN.

The limit represents the maximum number of distinct unicast MAC addresses that can be learnt in the VLAN. This value ranges between 0 and 4294967295. The maximum number of unicast MAC addresses that can be learnt differs for SMIS models. 0 is unlimited and determined by the underlying hardware.

This feature may not be supported because of hardware limits.

The maximum limit that can be configured for a VLAN is dependent on the total size available for dynamic unicast entries in the forwarding table and on the maximum number of VLANs that can be supported. The lower and upper limit values depend on the underlying hardware.

The no form of the command resets the unicast-MAC learning limit for the VLAN to its default value.

Syntax **vlan unicast-mac learning limit <size(0-4294967295)>**

no vlan unicast-mac learning limit

Mode Config-VLAN Mode

Default 0

Notes:

- VLAN unicast MAC learning limit configuration is allowed only in case of independent VLAN learning mode.
- VLAN unicast-MAC learning limit cannot be configured for the VLAN, if the base bridge mode is set as transparent bridging.
- The unicast-MAC learning limit set for the VLAN should not exceed the unicast MAC learning limit configured for the switch.
- VLAN unicast-MAC learning limit can be configured only in the VLANs that are activated.

Example

```
Your Product(config-switch-vlan)# vlan unicast-mac learning limit 100
```

Related Command(s)

- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `unicast-mac learning limit` - Configures the unicast-MAC learning limit for a switch.
- `vlan active` - Activates a VLAN in the switch.
- `show vlan learning params` - Displays the VLAN learning parameter details for all active VLANs and VLANs (that are not active) for which the port details are configured, available in all contexts / in the switch.

switchport pvid

Command Objective This command configures the PVID on the specified port. The PVID represents the VLAN ID that is to be assigned to untagged frames or priority-tagged frames received on the port. The PVID is used for port based VLAN type membership classification. This value ranges between 1 and 65535.

- `<vlan -id>` - This is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
- `<vfi-id>.` - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This is not supported.

Notes:

- The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
- VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
- The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted

in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

The PVID configuration done is used based on the acceptable frame type of the port. The packets are processed against PVID, if the packets accepted at ingress is not having a tag.

The no form of the command resets the PVID to the default value on the port.

Syntax **switchport pvid <vlan-id/vfi_id>**

no switchport pvid

Mode Interface Configuration mode (Physical / Port Channel)

Default 1 (ID of default VLAN)

Notes:

- Only the IDs of the active VLAN can be used as PVIDs in the command.
- This command is applicable only for the port configured as switch port.
- The PVID cannot be configured for the port, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.

Example

```
Your Product(config-if)# switchport pvid 3
```

Related Command(s)

- `switchport` - Configures the port as switch port.
- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `vlan active` - Activates a VLAN in the switch.
- `switchport acceptable-frame-type` - Configures the type of VLAN dependant BPDU frames such as GMRP BPDU, that the port should accept during the VLAN membership configuration.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan port config` - Displays the VLAN related port specific information for all interfaces available in the switch / all contexts.

switchport access vlan

Command Objective This command configures the PVID (Port VLAN Identifier) on a port. This value ranges between 1 and 4094.

The no form of this command sets the PVID to the default value on the port.

Notes:

- This command is a complete standardized implementation of the existing command and operates similar to that of the command switchport pvid.
- This feature has been included in adherence to the Industry Standard CLI syntax.

Syntax **switchport access vlan <vlanid (1-4094)>**

no switchport access vlan

Mode Interface Configuration Mode(Physical / Port Channel)

Notes:

- If the frame (untagged/priority tagged/customer VLAN tagged) is received on a "tunnel" port, then the default PVID associated with the port is used.
- If the received frame cannot be classified as MAC-based or port-and- protocol-based, then the PVID associated with the port is used.
- Usage is based on acceptable frame type of the port. Packets will be either dropped or accepted at ingress. Once a packet is accepted, if the packet is having a tag, it will be processed against that tag. Otherwise, the packet will be processed against PVID.

Example

```
Your Product(config-if)# switchport access vlan 3
```

Related Command(s)

- `show vlan port config` - Displays the VLAN related parameters specific for ports
- `switchport pvid` - Configures the PVID on the specified port

switchport acceptable-frame-type

Command Objective This command configures the type of VLAN dependent BPDU frames such as GMRP BPDU that the port should accept during the VLAN membership configuration.

The no form of the command resets the acceptable frame type for the port to its default value.

This configuration does not affect VLAN independent BPDU frames such as GVRP BPDU and STP BPDU. It affects only the VLAN dependent BPDU frames.

Syntax **switchport acceptable-frame-type {all | tagged | untaggedAndPrioritytagged}**

no switchport acceptable-frame-type

Parameter Description

- all - Configures the acceptable frame type as all. All tagged, untagged and priority tagged frames received on the port are accepted and subjected to ingress filtering.
- tagged - Configures the acceptable frame type as tagged.

  Only the tagged frames received on the port are accepted and subjected to ingress filtering. The untagged and priority tagged frames received on the port are rejected.

- untaggedAndPrioritytagged - Configures the acceptable frame type as untagged and priority tagged. Only the untagged or priority tagged frames received on the port are accepted and subjected to ingress filtering. The tagged frames received on the port are rejected.

Mode Interface Configuration Mode(Physical / Port Channel)

Default all

Notes:

- This command is applicable only for the port configured as switch port.
- The acceptable frame type cannot be configured for the port, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.
- The acceptable frame type cannot be configured and is always set as untaggedAndPrioritytagged, if the bridge port type is set as customer network port. The bridge port type can be set as CNP only in Metro package.

Example

```
Your Product(config-if)# switchport acceptable-frame-type tagged
```

Related Command(s)

- **switchport** - Configures the port as switch port.
- **bridge port-type** - Configures the bridge port type for an interface.
- base bridge-mode dot1q-vlan - Configures the VLAN operation mode as VLAN aware bridging.
- switchport pvid - Configures the PVID on the specified port.
- switchport ingress-filter - Enables ingress filtering feature on the port.
- switchport mode - Configures the mode of operation for a switch port.
- no shutdown vlan - Starts and enables VLAN switching feature in the switch.
- show vlan port config - Displays the VLAN related port specific information for all interfaces available in the switch / all contexts.

switchport ingress-filter

Command Objective This command enables ingress filtering feature on the port. The ingress filtering is applied for the incoming frames received on the port.

Only the incoming frames of the VLANs that have this port in its member list are accepted. This configuration does not affect VLAN independent BPDU frames such as GVRP BPDU and STP BPDU. It affects only the VLAN dependent BPDU frames GMRP BPDU.

The no form of the command disables ingress filtering feature on the port. All incoming frames received on the port are accepted.

Syntax **switchport ingress-filter**

no switchport ingress-filter

Mode Interface Configuration Mode(Physical / Port Channel)

Default The ingress filtering feature is disabled on the port.

Notes:

- This command is applicable only for the port configured as switch port.
- The ingress filtering cannot be configured on the port, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.
- The ingress-filtering feature cannot be configured and is always enabled on the port, if the bridge port type is set as customer network port – S tagged. The bridge port type can be set as CNP-S tagged only in Metro package.

Example

```
Your Product(config-if)# switchport ingress-filter
```

Related Command(s)

- `switchport` - Configures the port as switch port.
- `bridge port-type` - Configures the bridge port type for an interface.
- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `switchport acceptable-frame-type` - Configures the type of VLAN dependant BPDU frames such as GMRP BPDU, that the port should accept during the VLAN membership configuration.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan port config` - Displays the VLAN related port specific information for all interfaces available in the switch / all contexts.

port protocol-vlan

Command Objective This command enables protocol-VLAN based membership classification in a port. VLAN membership classification is done for all untagged and priority- tagged frames based on the port-protocol group / higher layer protocol for the port.

The no form of the command disables protocol-VLAN based membership classification in the port.

Syntax **port protocol-vlan**

no port protocol-vlan

Mode Interface Configuration Mode (Physical / Port Channel)

Default Protocol-VLAN based membership classification is enabled on all ports.

Notes:

- Protocol-VLAN based membership classification can be enabled or disabled in the ports without depending on the global status of the protocol-VLAN based membership classification.

- The change in global protocol-VLAN based membership classification overrides the port membership classification. For example, If the classification in the port is set as enabled while global classification is disabled, and if global classification is changed as enabled and once again to disabled, the classification in the port will be automatically set as disabled.
- Protocol-VLAN based membership classification can be enabled / disabled in the switch, only if the VLAN switching feature is started and enabled in the switch.

Example

```
Your Product(config-if)# no port protocol-vlan
```

Related Command(s)

- `protocol-vlan` - Enables protocol-VLAN based membership classification on all ports of the switch.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan port config` - Displays the VLAN related port specific information for all interfaces available in the switch / all contexts.

switchport map protocols-group

Command Objective This command maps the configured protocol group to a particular VLAN ID for an interface. This configuration is used during protocol-VLAN based membership classification.

The no form of the command deletes the entry created for the specified group ID in the Port Protocol Table.

Syntax **switchport map protocols-group <Group id integer(0-2147483647)> vlan <vlan-id/vfi_id>**

no switchport map protocols-group <Group id integer(0-2147483647)>

Parameter Description

- `<Group id integer(0-2147483647)>` - Configures a unique group ID that is already created with the specified protocol type and encapsulation frame type. This value represents a specific group that should be associated with a VID. This value ranges between 0 and 2147483647.
- `vlan <vlan-id/vfi-id>` - Maps the configured protocol group to the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - `<vfi-id>`. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

Notes:

- The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the

VID in management operations or Filtering Database entries.

  - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
  - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

Mode Interface Configuration Mode(Physical / Port Channel)

Notes:

- The protocol group should have been already created with a specific protocol and encapsulation frame type combination before mapping it to a VID.
- This command is applicable only for the port configured as switch port.
- The protocol group mapping cannot be configured for the port, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.

Example

```
Your Product(config-if)# switchport map protocols-group 1 vlan 2
```

Related Command(s)

- `switchport` - Configures the port as switch port.
- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `map protocol` - Creates a protocol group with a specific protocol and encapsulation frame type combination.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show protocol-vlan` - Displays all entries in the port protocol table.

switchport priority default

Command Objective This command configures the default ingress user priority for a port.

This priority is assigned to frames received on the port that does not have a priority assigned to it. This priority value is useful only on media such as Ethernet that does not support native user priority. This value ranges from 0 to 7. The value 0 represents the lowest priority and the value 7 represents the highest priority.

The no form of the command resets the default ingress user priority for the port to its default value.

Syntax **switchport priority default <priority value(0-7)>**

no switchport priority default

Mode Interface Configuration Mode (Physical / Port Channel)

Default 0

Notes:

- This command is applicable only for the port configured as switch port.
- The default user priority cannot be configured for the port, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.

Example

```
Your Product(config-if)# switchport priority default 5
```

Related Command(s)

- `switchport` - Configures the port as switch port.
- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan port config` - Displays the VLAN related port specific information for all interfaces available in the switch / all contexts.

switchport mode

Command Objective This command configures the mode of operation for a switch port. This mode defines the way of handling of traffic for VLANs.

The no form of the command resets the mode of operation for the switch port to its default value.

Syntax **switchport mode { access | trunk | hybrid | {private-vlan {promiscuous | host }} |{dynamic {auto | desirable}} }**

no switchport mode

Parameter Description

- `access` - Configures the port as access port that accepts and sends only untagged. This kind of port is added as a member to specific VLAN only and carries traffic only for the VLAN to which the port is assigned. The port can be set as access port, only if the following 3 conditions are met:
  - The GVRP is disabled for that port.
  - Acceptable frame type is set as “untagged AND priority” tagged.
  - Port is a not a tagged member of any VLAN.
- `trunk` - Configures the port as trunk port that accepts and sends only tagged frames. This kind of port is added as member of all existing VLANs and for any new VLAN created, and carries traffic for all VLANs. The trunk port accepts untagged frames too, if the acceptable frame type is set as all. The port can be set as trunk port, only if the port is not a member of untagged ports for any VLAN in the switch.
- `hybrid` - Configures the port as hybrid port that accepts and sends both tagged and untagged

frames.

- `private-vlan` - Configures Pvlan for the specified VLAN switch port.
- `promiscuous` - Communicates with all interfaces, including the isolated and community ports within a PVLAN. The function of the promiscuous port is to move traffic between ports in community or isolated VLANs.
- `host` - Specifies the type of a port in private vlan domain. Untagged member port in a primary or secondary vlan
  - If a host port is a member port of an isolated VLAN, traffic from the host port is sent only to the promiscuous port of the Private VLAN and the trunk port.
  - If a host port is a member port of the community VLAN, traffic from the port can be sent only to other ports of the community VLAN , trunk port and promiscuous port of the private VLAN.
- `dynamic` - Configures the mode as Dynamic Mode. This can be:
  - `auto`**–** Interface converts the link to a trunk link.
  - `desirable`**–** Interface actively attempts to convert the link to a trunk link.

    Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Interface Configuration Mode (Physical / Port Channel)

Default hybrid

Notes:

- This command is applicable only for the port configured as switch port.
- The VLAN port mode cannot be configured for the port, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.

Example

```
Your Product(config-if)# switchport mode access
```

Related Command(s)

- `spanning-tree guard`- Configures the various PVRST guard features such as root guard, in a port.
- `spanning-tree encap` - Configures the encapsulation type to be used in an interface.
- `switchport` - Configures the port as switch port.
- `base bridge-mode dot1q-vlan`- Configures the VLAN operation mode as VLAN aware bridging.
- `set port gvrp`- Enables or disables GVRP feature on the specified interface.
- `ports` - Statically configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN.
- `switchport acceptable-frame-type` - Configures the type of VLAN dependant BPDU frames such as GMRP BPDU, that the port should accept during the VLAN membership configuration.
- `switchport mode dot1q-tunnel`- Enables dot1q-tunneling on the specified interface
- `no shutdown vlan`- Starts and enables VLAN switching feature in the switch.
- `show vlan port config` - Displays the VLAN related port specific information for all interfaces

available in the switch / all contexts.

vlan max-traffic-class

Command Objective This command configures the maximum number of traffic classes supported on a port.

The number of traffic classes supported depends on the hardware used, which can limit the number of traffic classes to a lower number. SMIS supports eight traffic classes to handle priority traffic. Each traffic is assigned a traffic type based on the time sensitiveness of the traffic. This value ranges between 1 and 8.

The no form of the command resets the maximum traffic class value on the port to its default value.

Syntax **vlan max-traffic-class <MAX Traffic class(1-8)>**

no vlan max-traffic-class

Mode Interface Configuration Mode (Physical / Port Channel)

Default 8

Note: The maximum number of traffic classes supported on the port can be configured, only if the VLAN switching feature is started and enabled in the switch.

Example

```
Your Product(config-if)# vlan max-traffic-class 7
```

Related Command(s)

- `vlan map-priority` - Maps an evaluated user priority to a traffic class on a port.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.

vlan map-priority

Command Objective This command maps an evaluated user priority to a traffic class on a port.

The frame received on the interface with the configured priority is processed in the configured traffic class. Traffic class is used to meet the latency and throughput requirement of time-critical traffic in a LAN environment, where both time-critical and non-time-critical traffic compete for the network bandwidth.

The no form of the command maps the default traffic class to the specified priority value on the port.

Syntax **vlan map-priority <priority value(0-7)> traffic-class <Traffic class value(0-7)>**

no vlan map-priority <priority value (0-7)>

Parameter Description

- `<priority value(0-7)>` - Configures the priority value to be set for the specified traffic class. This value ranges between 0 and 7. The frames with the configured priority are mapped to the specified traffic class. The priority determined for the received frame is equivalent to the priority indicated in the received tagged frame or one of the evaluated priorities determined based on the media-type. The priority determined is equal to the Default User Priority value for the ingress port, if the untagged frames are received from Ethernet media. The priority determined is equal to the Regen user priority for the ingress port and media-specific user priority, if the untagged frames are received from non-Ethernet media.

- `<Traffic class value(0-7)>` - Configures the traffic class value to which the received frame of specified priority is to be mapped. This value ranges between 0 and 7. Each value represents the concerned traffic. They are:
    - 0 - Best effort. This represents all kinds of non-detrimental traffic that is not sensitive to QoS metrics such as jitter.
    - 1 - Background. This represents bulk transfers and other activities that are permitted on the network without impacting the network usage for users and applications.
    - 2 - Standard (spare traffic). This represents traffic of more importance than background but less importance than excellent load.
    - 3 - Excellent load. This represents the best effort type service that an information services organization should deliver to its most important customers.
    - 4 - Controlled load. This represents traffic subject to admission control to assure that the traffic is received even when the network is overloaded.
    - 5 - Interactive voice and video. This represents traffic having delay less than 100 milli-seconds.
    - 6 - Internetwork control-Layer 3 network control. This represents traffic having delay less than 10 milli-seconds.
    - 7 - Network control-Layer 2 network control reserved traffic. This represents traffic that demands special treatment based on its requirements and relative importance.

    The configured traffic class value should be less than the maximum number of traffic classes in the port.

Mode Interface Configuration Mode (Physical / Port Channel)

Default The default traffic classes that are mapped to the priority is listed below:

Priority	Traffic Class
1	0
2	1
3	3
4	4
5	5
6	6

7	7

Notes:

- The default traffic classes mapped to the priority value depends upon the maximum traffic classes supported on the port.
- The evaluated user priority can be mapped to the traffic class, only if the VLAN switching feature is started and enabled in the switch.

Example `Your Product(config-if)# vlan map-priority 2 traffic-class 2`

Related Command(s)

- `vlan max-traffic-class` - Configures the maximum number of traffic classes supported on a port.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan traffic-classes` - Displays the evaluated user priority and traffic class mapping information of all interfaces available in the switch / all contexts.

mac-map

Command Objective This command configures VLAN-MAC address mapping that is used only for MAC-based VLAN membership classification.

In MAC-based VLAN membership classification, VLAN membership classification is done based on the MAC address of the source of received packets.

The no form of the command deletes the specified VLAN-MAC address mapping entry.

Syntax **mac-map <aa:aa:aa:aa:aa:aa> vlan <vlan-id/vfi-id>**

no mac-map <aa:aa:aa:aa:aa:aa>

Parameter Description

- `<aa:aa:aa:aa:aa:aa>` - Configures the unicast MAC address that should be mapped to the specified VLAN and used for MAC based VLAN membership classification.
- `vlan <vlan-id/vfi-id>` - Maps the MAC Address to the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - `<vfi-id>`. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This is not supported.
    - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.

- VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
- The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of

  VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

Mode Global Configuration Mode

Notes:

- Only the VLANs that are activated in the switch can be mapped to the specified MAC address.
- VLAN-MAC address mapping can be configured in the port, only if the VLAN switching feature is started and enabled in the switch.

Example

```
Your Product(config)# mac-map 00:11:22:33:44:55 vlan 2
```

Related Command(s)

- `mac-vlan` - Enables MAC-based VLAN membership classification on all ports of the switch.
- `vlan active` - Activates a VLAN in the switch.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show mac-vlan` - Displays all entries in the MAC map table.

switchport filtering-utility-criteria

Command Objective This command creates filtering utility criteria for the port. This utility criteria is used to reduce the capacity requirement of the filtering database and to reduce the time for which service is affected, by retaining the filtering information learnt prior to a change in the physical topology of the network.

Syntax **switchport filtering-utility-criteria {default | enhanced}**

Parameter Description

- `default` - Allows learning of source MAC from a packet received on the port, only if there is at least one member port for a VLAN mentioned in the packet.
- `enhanced` - Allows learning of source MAC from a packet received on the port, only if the following conditions are satisfied:
  - At least one VLAN that uses the FID includes the reception port and at least one other Port with a port state of Learning or Forwarding in its member set.
  - The operPointToPointMAC parameter is false for the reception port. Or Ingress to the VLAN is permitted through a port other than source and reception. This port can be or not be in the member set for the VLAN.

Mode Interface Configuration Mode (Physical / Port Channel)

Default default

Notes:

- The filtering utility criteria cannot be configured in the switch, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.
- This command is applicable only for the port configured as switch port.

Example

```
Your Product(config-if)# switchport filtering-utility- criteria enhanced
```

Related Command(s)

- `switchport` - Configures the port as switch port.
- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan port config` - Displays the VLAN related port specific information for all interfaces available in the switch / all contexts

switchport protected

Command Objective This command enables switchport protection feature for a port.

This feature set the particular port as protected so that the port does not forward frames received from another protected port present on the same switch.

The no form of the command disables switchport protection feature for the port.

Syntax **switchport protected**

no switchport protected

Mode Interface Configuration Mode (Physical / Port Channel)

Default The switchport protection feature is disabled in the port.

Notes:

- The switchport protection feature cannot be configured in the switch, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.
- This command is applicable only for the port configured as switch port.

Example

```
Your Product(config-if)# switchport protected
```

Related Command(s)

- `switchport` - Configures the port as switch port.
- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan port config` - Displays the VLAN related port specific information for all interfaces available in the switch / all contexts.

debug vlan

Command Objective This command enables the tracing of the VLAN sub module as per the configured debug levels. The trace statements are generated for the configured trace levels.

The no form of the command disables the tracing of the VLAN sub module as per the configured debug levels. The trace statements are not generated for the configured trace levels.

This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled).

Syntax **debug vlan { [{fwd | priority | redundancy}([initshut] [mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all])] [switch <context_name>] }**

no debug vlan {[{fwd | priority | redundancy}([initshut] [mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all])] [switch <context_name>]}

Parameter Description

- `fwd` - Sets the submodule as VLAN forward module, for which the tracing is to be done as per the configured debug levels.
- `priority` - Sets the submodule as VLAN priority module, for which the tracing is to be done as per the configured debug levels.
- `redundancy` - Sets the submodule as VLAN redundancy module, for which the tracing is to be done as per the configured debug levels.
- `initshut` - Generates debug statements for init and shutdown traces. This trace is generated on failed initialization and shutting down of VLAN related entries.
- `mgmt` - Generates debug statements for management traces. This trace is generated during failure in configuration of any of the VLAN features.
- `data` - Generates debug statements for data path traces. This trace is generated during failure in packet processing.
- `ctpl` - Generates debug statements for control path traces. This trace is generated during failure in modification or retrieving of VLAN entries.
- `dump` - Generates debug statements for packet dump traces. This trace is currently not used in VLAN module.
- `os` - Generates debug statements for OS resource related traces. This trace is generated during failure in message queues.
- `failall` - Generates debug statements for all kind of failure traces.
- `buffer` - Generates debug statements for VLAN buffer related traces. This trace is currently not

used in VLAN module.

- `all` - Generates debug statements for all kinds of traces.
- `switch <context_name>` - Configures the tracing of the VLAN submodule for the specified context. This value represents unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.

Mode Privileged Exec Mode

Default Tracing of the VLAN sub module is disabled.

Note: The VLAN sub module tracing related configuration takes effect in the switch, only if the VLAN switching feature is started and enabled in the switch.

Example

```
Your Product# debug vlan fwd all
```

Related Command(s)

- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show debugging` - Displays state of each debugging option.

show vlan

Command Objective This command displays VLAN entry related information of all active VLANs and VLANs (that are not active) for which the port details are configured.

The information contains the member ports, untagged ports, forbidden ports, VLAN name and the status of that VLAN entry.

Syntax **show vlan [{brief | id <vlan-range> | summary | redundancy| ascending}] [switch <context_name>]**

Parameter Description

- `brief` - Displays the VLAN entry related information of all active VLANs and VLANs (that are not active) for which the port details are configured.
- `id <vlan-range>` - Displays the VLAN entry related information for specified VLANs alone. This value denotes the VLAN ID range for which the information needs to be displayed. This value is a string whose maximum size is 9. For example, the value is provided as 4000-4010 to display the information for VLANs IDs from 4000 to 4010. The information is displayed only for the active VLANs and VLANs (that are not active) for which the port details are configured.
- `summary` - Displays only the total number of VLANs existing in the switch. This includes only the active VLANs and VLANs (that are not active) for which the port details are configured. The VLAN entry related information is not displayed.
- `redundancy` - Displays the VLAN entry related information for standby node.
- `ascending` - Displays the VLAN entry related information in ascending order.
- `switch <context_name>` - Displays the VLAN entry related information or total number of existing VLANs, for the specified context. This value represents unique name of the switch context. This value

is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show vlan brief
Vlan database
--------------------
Vlan ID      : 1
Member Ports :             Gi0/1, Gi0/2, Gi0/3, Gi0/4, Gi0/5, Gi0/6
Gi0/7, Gi0/8, Gi0/9, Gi0/10, Gi0/11, Gi0/12
Gi0/13, Gi0/14, Gi0/15, Gi0/16, Gi0/17,
Gi0/18
Gi0/19, Gi0/20, Gi0/21, Gi0/22, Gi0/23,
Gi0/24
Untagged Ports:          Gi0/1, Gi0/2, Gi0/3, Gi0/4, Gi0/5, Gi0/6
Gi0/7, Gi0/8, Gi0/9, Gi0/10, Gi0/11, Gi0/12
Gi0/13, Gi0/14, Gi0/15, Gi0/16, Gi0/17,
Gi0/18
Gi0/19, Gi0/20, Gi0/21, Gi0/22, Gi0/23,
Gi0/24
Forbidden Ports             : None
Name                              :
Status                            : Permanent
--------------------------------------------------------------------------------
Your Product# show vlan summary
Number of vlans : 1
```

Related Command(s)

- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `vlan` - Creates a VLAN in the ISS and enters into the config-VLAN mode in which VLAN specific configurations are done.
- `ports` - Statically configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN.
- `vlan active` - Activates a VLAN in the switch.

show vlan device info

Command Objective This command displays the VLAN global information that is applicable to all VLANs created in the switch / all contexts.

The information contains VLAN status, VLAN oper status, GVRP status, GMRP status, GVRP oper status, GMRP oper status, MAC-VLAN status, subnet-VLAN status, protocol-VLAN status, bridge mode of the switch, VLAN base bridge mode, VLAN traffic class status, VLAN learning mode, VLAN version number, maximum VLAN ID supported, maximum number of VLANs supported and VLAN unicast MAC learning limit.

Syntax **show vlan device info [switch <context_name>]**

Parameter Description `switch <context_name>` - Displays the VLAN global information that is applicable to all VLANs, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. For the models without multiple instance feature, it is not required to provide this parameter.

Mode Privileged EXEC Mode

Example

```
Your Product# show vlan device info
Vlan device configurations
---------------------------------------
Vlan Status                          : Enabled
Vlan Oper status                     : Enabled
Gvrp status                          : Enabled
Gmrp status                          : Disabled
Gvrp Oper status                     : Enabled
Gmrp Oper status                     : Disabled
Mac-Vlan Status                      : Disabled
Subnet-Vlan Status                   : Enabled
Protocol-Vlan Status                 : Enabled
Bridge Mode                          : Customer Bridge
Base-Bridge Mode                     : Vlan Aware Bridge
Traffic Classes                      : Enabled
Vlan Operational Learning Mode       : IVL
Version number                       : 1
Max Vlan id                          : 4094
Max supported vlans                  : 1024
Unicast mac learning limit           : 150
Filtering Utility Criteria           : Enabled
Unicast mac learning limit           : 768
```

Related Command(s)

- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `set vlan` - Globally enables / disables VLAN feature in the switch (that is the status of the VLAN feature is configured for all ports of the switch).
- `set gvrp` - Globally enables / disables GVRP feature on all ports of a switch.
- `set gmrp` - Globally enables / disables GMRP feature on all ports of a switch.
- `mac-vlan` - Enables MAC-based VLAN membership classification on all ports of the switch.
- `subnet-vlan` - Enables subnet-VLAN based membership classification on all ports of the switch.
- `protocol-vlan` - Enables protocol-VLAN based membership classification on all ports of the switch.
- `base bridge-mode` - Configures the base mode (either 802.1d transparent bridge mode or 802.1q vlan aware bridge mode) in which the VLAN feature should operate on the switch.
- `set vlan traffic-classes` - Enables or disables traffic class feature in a switch on all ports.
- `vlan learning mode` - Configures the VLAN learning mode to be applied for all ports of the switch.
- `unicast-mac learning limit` - Configures the unicast-MAC learning limit for a switch.

- `set filtering-utility-criteria` - Sets the filtering utility criteria to be applied on all ports

show vlan device capabilities

Command Objective This command displays only the list of VLAN features such as traffic classfeature, supported in the switch / all contexts.

Syntax **show vlan device capabilities [switch <context_name>]**

Parameter Description `switch <context_name>` - Displays only the list of supported VLAN features such as traffic class feature, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature. It is not necessary to provide this parameter for the models without multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product#
show vlan device capabilities
Vlan device capabilities
-------------------------- Extended filtering services Traffic classes
Static Entry Individual port
IVL capable SVL capable Hybrid capable
Configurable Pvid Tagging
```

Related Command(s) `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.

show vlan traffic-classes

Command Objective This command displays the evaluated user priority and traffic class mapping information of all interfaces available in the switch / all contexts.

Syntax **show vlan traffic-classes [{port <interface-type><interface-id> | switch <context_name>}]**

Parameter Description

- `port` - Displays the evaluated user priority and traffic class mapping information of the specified interface. The details to be provided are:
    - `<interface-type>` - Sets the type of interface. The interface can be:
        - `fastethernet` – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
        - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

- `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
- `i-lan`– Internal LAN created on a bridge per IEEE 802.1ap.

- `<interface-id>` - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan. Only i-lan ID is provided, for interface type i- lan.

- `switch <context_name>` - Displays the evaluated user priority and traffic class mapping information of all interfaces, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

Single Instance:

```
Your Product# show vlan traffic-classes
Traffic Class table
---------------------------------
Port                       Priority            Traffic Class
                           -----------------   -------------------------

Gi0/1                      0             2
Gi0/1                      1             0
Gi0/1                      2             1
Gi0/1                      3             3
Gi0/1                      4             4
Gi0/1                      5             5
Gi0/1                      6             6
Gi0/1                      7             7
Gi0/2                      0             2
Gi0/2                      1             0
Gi0/2                      2             1
Gi0/2                      3             3
Gi0/2                      4             4
Gi0/2                      5             5
Gi0/2                      6             6
Gi0/2                      7             7
```

Related Command(s)

- `vlan map-priority` - Maps an evaluated user priority to a traffic class on a port.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.

show vlan port config

Command Objective This command displays the VLAN related port specific information for all interfaces available in the switch / all contexts. The information contains PVID, acceptable frame type, port mode, filtering utility criteria, default priority value and status of ingress filtering feature, GVRP module, GMRP module, restricted VLAN registration feature, restricted group registration feature, MAC-based VLAN membership, subnet based VLAN membership, protocol-VLAN based membership and port protected feature.

Syntax **show vlan port config [{port <interface-type> <interface- id> | switch <context_name>}]**

Parameter Description

- `port` - Displays the VLAN related port specific information for the specified interface. The details to be provided are:
  - `<interface-type>` - Sets the type of interface. The interface can be:
    - `fastethernet` – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Megabits per second.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `internal-lan` – Internal LAN created on a bridge per IEEE 802.1ap.
    - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
    - `virtual` – Virtual Interface. This value ranges from 1 to 65535.
  - <interface-id> - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel.
- `switch <context_name>` - Displays the VLAN related port specific information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show vlan port config
Vlan Port configuration table
-------------------------------------------------
Port Gi0/1
Port Vlan ID                                   : 1
Port Acceptable Frame Type              : Admit All
Port Ingress Filtering                  : Disabled
Port Mode                                      : Hybrid
Port Gvrp Status                        : Enabled
Port Gmrp Status                        : Enabled
Port Gvrp Failed Registrations                 : 0
```

```
Gvrp last pdu origin                    : 00:00:00:00:00:0
Port Restricted Vlan Registration       : Disabled
Port Restricted Group Registration             : Disabled
Mac Based Support                       : Disabled
Subnet Based Support                    : Disabled
Port-and-Protocol Based Support         : Enabled
Default Priority                               : 0
Filtering Utility Criteria                     : Default
Port Protected Status                   : Disabled
----------------------------------------------------------------------------------
Port Gi0/2
Port Vlan ID                                   : 1
Port Acceptable Frame Type              : Admit All
Port Ingress Filtering                  : Disabled
Port Mode                                      : Hybrid
Port Gvrp Status                        : Enabled
Port Gmrp Status                        : Enabled
Port Gvrp Failed Registrations                 : 0
Gvrp last pdu origin                    : 00:00:00:00:00:00
Port Restricted Vlan Registration       : Disabled
Port Restricted Group Registration             : Disabled
Mac Based Support                       : Disabled
Subnet Based Support                    : Disabled
Port-and-Protocol Based Support         : Enabled
Default Priority                               : 0
Filtering Utility Criteria                     : Default
Port Protected Status                   : Disabled
```

Related Command(s)

- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `switchport pvid` - Configures the PVID on the specified port.
- `switchport acceptable-frame-type` - Configures the type of VLAN dependant BPDU frames such as GMRP BPDU, that the port should accept during the VLAN membership configuration.
- `switchport ingress-filter` - Enables ingress filtering feature on the port.
- `switchport mode` - Configures the mode of operation for a switch port.
- `set port gvrp` - Enables or disables GVRP feature on the specified interface.
- `set port gmrp` - Enables or disables GMRP feature on the specified interface.
- `vlan restricted` - Configures the restricted VLAN registration feature in a port.
- `group restricted` - Configures the restricted group registration feature in a port.
- `port protocol-vlan` - Enables protocol-VLAN based membership classification in a port.
- `switchport priority default` - Configures the default ingress user priority for a port.
- `switchport filtering-utility-criteria` - Creates filtering utility criteria for the port.
- `switchport protected` - Enables switchport protection feature for a port.

show vlan protocols-group

Command Objective This command displays all entries in the protocol group table. These entries contain protocol group information of the switch / all contexts. The information contain ID of a group, protocol assigned to the group, and frame type assigned to the group.

Syntax **show vlan protocols-group [switch <context_name>]**

Parameter Description `switch <context_name>`- Displays all entries in the protocol group table, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show vlan protocols-group
Protocol Group Table
-----------------------------------------

---------------------------------------------------------------------
Frame Type                    Protocol        Group
---------------------------------------------------------------------
Enet-v2                         IP            1
Snap                            Novell        2
```

Related Command(s)

- `map protocol` - Creates a protocol group with a specific protocol and encapsulation frame type combination.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.

show protocol-vlan

Command Objective This command displays all entries in the port protocol table. These entries contain VLAN-protocol group mapping information of the switch / all contexts. The information contains ID of a group, ID of a VLAN mapped to the group and ID of interface to which the VLAN-protocol group mapping is assigned.

Syntax **show protocol-vlan [switch <context_name>]**

Parameter Description `switch <context_name>` - Displays all entries in the port protocol table, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show protocol-vlan
Port Protocol Table
------------------------------------------------------------------------------
Port                            Group         Vlan ID
------------------------------------------------------------------------------
Gi0/2                           1             2
Gi0/1                           2             3
```

Related Command

- switchport map protocols-group - Maps the configured protocol group to a particular VLAN ID for an interface.
- no shutdown vlan - Starts and enables VLAN switching feature in the switch.

show mac-vlan

Command Objective This command displays all entries in the MAC map table. These entries contain MAC-VLAN mapping details configured for the interfaces available in the switch/ all contexts. The details contain MAC address, ID of VLAN that is mapped to the MAC address, multicast and broadcast status, and MAC-based VLAN membership status.

Syntax show mac-vlan [{interface <interface-type> <interface-id> |switch <string(32)>}]

Parameter Description

- interface - Displays all entries in the MAC map table for the specified interface. The details to be provided are:
  - <interface-type> - Sets the type of interface. The interface can be:
    - qx-ethernet – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
  - <interface-id> - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID isprovided, for interface type port-channel.
- switch <string(32)> - Displays all entries in the MAC map table, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show mac-vlan interface gigabitethernet 0/1
Mac Map Table For Port 1--Mac Vlan Disabled
```

```
---------------------------------------------------
Mac Address        Vlan ID         MCast/Bcast
-------------------------------------------------         ---------------------
00:11:11:11:11:11    1             discard
00:22:22:22:22:22    1             allow
```

Related Command(s)

- `mac-vlan` - Enables MAC-based VLAN membership classification on all ports of the switch.
- `mac-map` - Configures the VLAN-MAC address mapping that is used only for MAC-based VLAN membership classification.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.

show subnet vlan mapping

Command Objective This command displays all entries in the subnet map table. These entries contain VLAN-IP subnet address mapping details configured for the interfaces available in the switch / all contexts. The details contain subnet address, ID of VLAN that is mapped to the subnet address, ARP status, and subnet-based VLAN membership status.

Syntax **show subnet-vlan mapping**

Mode Privileged EXEC Mode

Example

```
Your Product# show subnet-vlan mapping
Subnet Map Table For Port 1--Subnet Vlan Enabled
----------------------------------------------------------------------------------------------------------------------
Source IP                Subnet Mask      Vlan ID       ARP Traffic
----------------------------------------------------------------------------------------------------------------------
1.1.1.1                  255.0.0.0        4150          allow
```

Related Command(s)

- `subnet-vlan` - Enables subnet-VLAN based membership classification on all ports of the switch.
- `map subnet` - Configures VLAN-IP subnet address mapping that is used only for subnet-VLAN based membership classification.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.

show vlan statistics

Command Objective This command displays the unicast / broadcast statistics details of all active VLANs and VLANs (that are not active) for which the port details are configured.

The statistics details include VLAN ID, number of unicast packets received in the VLAN, number of multicast / broadcast packets received in the VLAN, number of unknown unicast packets flooded in the VLAN, number of known unicast packets forwarded in the VLAN, and number of known broadcast packets forwarded in the VLAN.

Syntax **show vlan statistics [vlan <vlan-range>] [switch <context_name>]**

Parameter Description

- vlan <vlan-range> - Displays the unicast / broadcast statistics details for specified VLANs alone. This value denotes the VLAN ID range for which the details need to be displayed. This value is a string whose maximum size is 9. For example, the value is provided as 4000-4010 to display the details for VLAN IDs from 4000 to 4010. The details are displayed only for the VLANs that are activated and VLANs (that are not active) for which the port details are configured.
- switch <context_name> - Displays the unicast / broadcast statistics details of specified VLANs alone or of all active VLANs and VLANs (that are not active) for which the port details are configured, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show vlan statistics vlan 1
Software Statistics Enabled
Unicast/broadcast Vlan statistics
-----------------------------------------------------------------------
Vlan Id                          : 1
Unicast frames received          : 0
Mcast/Bcast frames received      : 0
Unknown Unicast frames flooded   : 0
Unicast frames transmitted       : 0
Broadcast frames transmitted     : 0
Vlan Statistics Collection is Disabled
-----------------------------------------------------------------------
```

Related Command(s)

- vlan active - Activates a VLAN in the switch.
- ports - Statically configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN.
- clear vlan statistics - Clears VLAN counters that maintain statistics information on a per VLAN basis. The counter is cleared for all available VLANs or for the specified VLAN.
- no shutdown vlan - Starts and enables VLAN switching feature in the switch.
- set sw-stats - Sets the software statistics collection globally in the switch
- set vlan counter - Enables or disables the statistics collection for the specified VLAN.

show vlan learning params

Command Objective This command displays the VLAN learning parameter details for all active

VLANs and VLANs (that are not active) for which the port details are configured, available in all contexts /

in the switch. The details include admin status of unicast MAC learning feature and value representing MAC learning limit and operational status of learning feature.

Syntax **show vlan learning params [vlan <vlan-range>] [switch <string(32)>]**

Parameter Description

- `vlan <vlan-range>` - Displays the VLAN learning parameter details for specified VLANs alone. This value denotes the VLAN ID range for which the details need to be displayed. This value is a string whose maximum size is 9. For example, the value is provided as 4000-4010 to display the details for VLAN IDs from 4000 to 4010. The details are displayed only for the VLANs that are activated and VLANs (that are not active) for which the port details are configured.
- `switch <string(32)>` - Displays the VLAN learning parameter details of specified VLANs alone or of all active VLANs and VLANs (that are not active) for which the port details are configured, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode **Privileged EXEC Mode**

Example

Single Instance

```
Your Product# show vlan learning params
Unicast MAC Learning Paramters
------------------------------------------------------------
Vlan Id                  : 1
Mac Learning Admin-Status : Enable
Mac Learning Oper-Status : Enable
Mac Learning Limit        : 150
------------------------------------------------------------
```

Related Command(s)

- `vlan active` - Activates a VLAN in the switch.
- `ports` - Statically configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN.
- `set unicast-mac learning` - Enables or disables unicast-MAC learning feature for a VLAN.
- `vlan unicast-mac learning limit` - Configures the unicast-MAC learning limit for a VLAN.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.

show mac-address-table

Command Objective This command displays all static / dynamic unicast and multicast MAC entries created in the MAC address table. These entries contain VLAN ID, unicast / multicast MAC address, unicast backbone MAC address of peer backbone edge bridge, member ports, the type of entry (that is static, learnt and so on), and total number of entries displayed.

Syntax **show mac-address-table {[[vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> | switch <context_name> }]] | [redundancy] }**

Parameter Description

- `vlan <vlan-range>` - Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified VLANs alone. This value denotes the VLAN ID range for which the entries need to be displayed. This value is a string with the maximum size as 9. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to 4010.
- `address <aa:aa:aa:aa:aa:aa>` - Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified unicast / multicast MAC address.
- `interface` - Displays all static / dynamic unicast and multicast MAC entries for the specified interface. The details to be provided are:
    - <interface-type> - Sets the type of interface. The interface can be:
        - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
        - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
        - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
        - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
    - `<interface-id>` - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel.
- `switch <context_name>` - Displays all static / dynamic unicast and multicast MAC entries, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.
- `redundancy` - Displays all static / dynamic unicast and multicast MAC entries for standby node.

Mode Privileged EXEC Mode

Example

```
Your Product# show mac-address-table
Vlan
Ports                   Mac Address            Type         ConnectionId
----                    -----------            ----         ------------
--
1                        00:10:00:00:00:07     Learnt
Gi0/1
2                        00:10:00:01:02:03     Learnt
Gi0/1
Total Mac Addresses displayed: 2
```

Related Command(s) `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.

show dot1d mac-address-table

Command Objective This command displays all static / dynamic unicast and multicast MAC address entries created in the FDB table, when the VLAN base bridge mode is transparent bridging.

These entries contain unicast / multicast MAC address, member ports, and the type of entry (that is static, learnt and so on).

Syntax **show dot1d mac-address-table [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> | switch <context_name>}]**

Parameter Description

- `address <aa:aa:aa:aa:aa:aa>` - Displays all static / dynamic unicast and multicast MAC entries created in the FDB table for the specified unicast / multicast MAC address.
- `interface` - Displays all static / dynamic unicast and multicast MAC entries for the specified interface. The details to be provided are:
  - `<interface-type>` - Sets the type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
  - `<interface-id>` - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID isprovided, for interface type port-channel.
- `switch <context_name>` - Displays static / dynamic unicast and multicast MAC entries for the specified MAC address alone or all entries in the FDB table, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show dot1d mac-address-table
Mac Address               Type      Ports
-----------               ----      -----
```

```
00:00:d1:20:18:d4       Learnt   Gi0/1
Total Mac Addresses displayed: 1
```

Related Command(s)

- `mac-address-table static unicast` – Transparent Bridging Mode - Configures a static unicast MAC address in the forwarding database in transparent bridging mode in order to control unicast packets to be processed.
- `mac-address-table static multicast` – Transparent Bridging mode - Configures a static multicast MAC address in the forwarding database in transparent bridging mode in order to control multicast packets to be processed.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.

show mac-address-table count

Command Objective This command displays the total number of static / dynamic unicast and multicast MAC address entries created in the FDB table. The count is displayed for all active VLANs, VLANs (that are not active) for which the port details are configured, and VLANs for which the MAC address table entries are created.

Syntax **show mac-address-table count [vlan <vlan-id/vfi-id>] [switch <context_name>]**

Parameter Description

- vlan <vlan-id/vfi-id> - Displays the total number of static / dynamic unicast and multicast MAC address entries created for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - <vlan **–**id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.
    - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
    - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
    - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- switch <context_name> - Displays the total number of static / dynamic unicast and multicast MAC address entries, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show mac-address-table count
Mac Entries for Vlan 1:
---------------------------------------------------------------
Dynamic Unicast Address Count    : 0
Dynamic Multicast Address Count : 0
Static Unicast Address Count     : 0
Static Multicast Address Count   : 0
---------------------------------------------------------------------------
Mac Entries for Vlan 4099:
---------------------------------------------------------------
Dynamic Unicast Address Count    : 0
Dynamic Multicast Address Count : 0
Static Unicast Address Count     : 1
Static Multicast Address Count   : 0
---------------------------------------------------------------------------
Mac Entries for Vlan 4158:
---------------------------------------------------------------
Dynamic Unicast Address Count    : 0
Dynamic Multicast Address Count : 0
Static Unicast Address Count     : 0
Static Multicast Address Count   : 0
---------------------------------------------------------------------------
```

Related Command(s)

- `vlan active` - Activates a VLAN in the switch.
- `ports` - Statically configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.

show mac-address-table static unicast

Command Objective This command displays all static unicast MAC address entries created in the FDB table.

These entries contain VLAN ID to which unicast MAC address entry is assigned, unicast MAC address, member ports, receiver ports, the status of entry (that is permanent, static and so on), the unicast backbone MAC address of peer backbone edge bridge, and total number of entries displayed.

Syntax **show mac-address-table static unicast [vlan <vlan-range>] [address<aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> | switch <context_name>}]**

Parameter Description

- `vlan <vlan-range>` - Displays all static unicast MAC address entries created in the FDB table for the specified VLANs alone. This value denotes the VLAN ID range for which the entries need to be displayed. This value is a string whose maximum size is 9. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to 4010.

- `address <aa:aa:aa:aa:aa:aa>` - Displays all static unicast MAC address entries created in the FDB table for the specified unicast MAC address.
- `interface` - Displays all static unicast MAC address entries for the specified interface. The details to be provided are:
    - <interface-type> - Sets the type of interface. The interface can be:
        - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
        - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
        - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
        - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
    - `<interface-id>` - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel.
- `switch <context_name>` - Displays all static unicast MAC entries, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show mac-address-table static unicast
Vlan
Ports                    Mac Address            RecvPort      Status        ConnectionId
----                     -----------            --------      ------        -------------
2                        00:11:22:33:44:55     Gi0/2         Del-OnTimeout
Gi0/3
Total Mac Addresses displayed: 1
```

Related Command(s) `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.

show dot1d mac-address-table static unicast

Command Objective This command displays all static unicast MAC address entries created in the FDB table, when the VLAN base bridge mode is transparent bridging.

These entries contain unicast MAC address, member ports, receiver ports, the status of entry (that is permanent, static and so on), and total number of entries displayed.

Syntax **show dot1d mac-address-table static unicast [address <aa:aa:aa:aa:aa:aa>] [interface <interface-type> <interface-id>]**

Parameter Description

- `address <aa:aa:aa:aa:aa:aa>` - Displays all static unicast MAC entries created in the FDB table for the specified unicast MAC address.
- `interface-type` - Displays all static unicast MAC entries for the specified interface. The details to be provided are:
  - `<interface-type>` - Sets the type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
  - `<interface-id>` - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID isprovided, for interface type port-channel.

Mode Privileged EXEC Mode

Example

```
Your Product# show dot1d mac-address-table static unicast address 00:11:22:33:44:55
Mac Address               RecvPort        Status        Ports
-----------               --------        ------        -----
00:11:22:33:44:55                         Permanent     Gi0/2
Total Mac Addresses displayed: 1
```

Related Command(s)

- `mac-address-table static unicast –Transparent Bridging Mode` - Configures a static unicast MAC address in the forwarding database in transparent bridging mode in order to control unicast packets to be processed.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.

show mac-address-table static multicast

Command Objective This command displays the static multicast MAC address entries created in the

FDB table.

These entries contain VLAN ID to which multicast MAC address entry is assigned, multicast MAC address, member ports, receiver ports, forbidden ports, the status of entry (that is permanent, static and so on), and total number of entries displayed.

Syntax **show mac-address-table static multicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> | switch <context_name>}]**

Parameter Description

- `vlan <vlan-range>` - Displays all static multicast MAC address entries created in the FDB table for the specified VLANs alone. This value denotes the VLAN ID range for which the entries need to be displayed. This value is a string whose maximum size is 9. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to 4010.
- `address <aa:aa:aa:aa:aa:aa>` - Displays all static multicast MAC address entries created in the FDB table for the specified unicast MAC address.
- `interface` - Displays all static multicast MAC address entries for the specified interface. The details to be provided are:
    - `<interface-type>` - Sets the type of interface. The interface can be:
        - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
        - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
        - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
        - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
    - `<interface-id>` - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID isprovided, for interface type port-channel.
- `switch <context_name>` - Displays all static multicast MAC entries, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show mac-address-table static multicast
Static Multicast Table
-----------------------------------
Vlan                          : 1
```

```
Mac Address                    : 01:02:03:04:05:06
Receive Port                   : Gi0/1
Member Ports                   : Gi0/1
Forbidden Ports                : Gi0/2
Status                         : Permanent
------------------------------------------------------------------------
Total Mac Addresses displayed: 1
```

Related Command(s) no shutdown vlan - Starts and enables VLAN switching feature in the switch.

show dot1d mac-address-table static multicast

Command Objective This command displays all static multicast MAC address entries created in the FDB table, when the VLAN base bridge mode is transparent bridging.

These entries contain multicast MAC address, member ports, receiver ports, the status of entry (that is permanent, static and so on), and total number of entries displayed.

Syntax **show dot1d mac-address-table static multicast [address <aa:aa:aa:aa:aa:aa>] [interface <interface-type> <interface-id>]**

Parameter Description

- address <aa:aa:aa:aa:aa:aa> - Displays all static multicast MAC entries created in the FDB table for the specified multicast MAC address.
- interface - Displays all static multicast MAC entries for the specified interface. The details to be provided are:
  - <interface-type> - Sets the type of interface. The interface can be:
    - qx-ethernet –A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
  - <interface-id> - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID isprovided, for interface type port-channel.

Mode Privileged EXEC Mode

Example

```
Your Product# show dot1d mac-address-table static multicast address 01:00:5E:01:02:03
----------------------------       -------------    -------   --------
```

```
Mac Address                RecvPort     Type         Ports
01:00:5E:01:02:03                       static       Gi0/2-3
Total Mac Addresses displayed: 1
Your Product# show dot1d mac-address-table static multicast interface gigabitethernet
0/2
Mac Address                RecvPort     Type         Ports
---------------------------  -------------  --------     ----------
01:00:5E:01:02:03                       static       Gi0/2
01:00:5E:01:02:04          --------     static       Gi0/2
Total Mac Addresses displayed: 2
```

Related Command(s)

- `mac-address-table static multicast` – Transparent Bridging mode- Configures a static multicast MAC address in the forwarding database in transparent bridging mode in order to control multicast packets to be processed.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.

show mac-address-table dynamic unicast

Command Objective This command displays all dynamically learnt unicast entries from the MAC address table.

These entries contain VLAN ID for which unicast MAC address entry is learnt, unicast MAC address, ports through which the entry is learnt, the status of entry (that is permanent, static and so on), the unicast backbone MAC address of peer backbone edge bridge, and total number of entries displayed.

Syntax **show mac-address-table dynamic unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> | switch <context_name>}]**

Parameter Description

- `vlan <vlan-range>` - Displays all dynamically learnt unicast entries from the MAC address table for the specified VLANs alone. This value denotes the VLAN ID range for which the entries need to be displayed. This value is a string whose maximum size is 9. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to 4010.
- `address <aa:aa:aa:aa:aa:aa>` - Displays all dynamically learnt unicast entries from the MAC address table for the specified unicast MAC address.
- `interface` - Displays all dynamically learnt unicast entries from the MAC address table for the specified interface. The details to be provided are:
    - `<interface-type>` - Sets the type of interface. The interface can be:
        - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
        - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

  - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel.
- `switch <context_name>` - Displays all dynamically learnt unicast entries, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show mac-address-table dynamic unicast vlan 2
Vlan                     Mac Address            Type         ConnectionId Ports
----                     -----------     ----   ------       -----------
2                        00:01:02:03:04:21      Learnt       Gi0/1
Total Mac Addresses displayed: 1
```

Related Command(s) `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.

show mac-address-table dynamic multicast

Command Objective This command displays all dynamically learnt multicast entries from the MAC address table.

These entries contain VLAN ID for which multicast MAC address entry is learnt, multicast MAC address, ports through which the entry is learnt, the status of entry (that is permanent, static and so on), the unicast backbone MAC address of peer backbone edge bridge, and total number of entries displayed.

Syntax **show mac-address-table dynamic multicast [vlan <vlan- range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> | switch <context_name>}]**

Parameter Description

- `vlan <vlan-range>` - Displays all dynamically learnt multicast entries from the MAC address table for the specified VLANs alone. This value denotes the VLAN ID range for which the entries need to be displayed. This value is a string whose maximum size is 9. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to 4010.
- `address <aa:aa:aa:aa:aa:aa>`- Displays all dynamically learnt multicast entries from the MAC address table for the specified unicast MAC address.
- `interface` - Displays all dynamically learnt multicast entries from the MAC address table

for the specified interface. The details to be provided are:

  - `<interface-type>` - Sets the type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
  - `<interface-id>` - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel.
- `switch <context_name>` - Displays all dynamically learnt multicast entries, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature

Mode Privileged EXEC Mode

Example

```
Your Product# show mac-address-table dynamic multicast
Vlan                    Mac Address           Type   ConnectionId  Ports
----                    -----------           ----   ------------  -----
2                       01:03:05:07:09:04     Learnt               Gi0/1
Total Mac Addresses displayed: 1
```

Related Command(s) `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.

show mac-address-table aging-time

Command Objective This command displays the ageing time configured for the MAC address table.

This time denotes the interval (in seconds) after which the dynamically learned forwarding information entry and static entry in the MAC address table are deleted.

Syntax **show mac-address-table aging-time [switch <context_name>]**

Parameter Description `switch <context_name>`- Displays ageing time of the MAC address table, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show mac-address-table aging-time
Mac Address Aging Time: 300
```

Related Command(s)

- mac-address-table aging-time - Configures the timeout period (in seconds) for aging out dynamically learned forwarding information entry and static entry in the MAC address table.
- no shutdown vlan - Starts and enables VLAN switching feature in the switch.

show wildcard

Command Objective This command displays all wildcard MAC entries created in the switch / in all contexts.

The wild card VLAN static filtering information is used for all VLANs for which no static unicast and multicast MAC address entries are created.

Syntax **show wildcard {mac-address <mac_addr> | broadcast} [switch <context_name>]**

Parameter Description

- mac-address <mac_addr> - Displays the wildcard MAC entries created in the switch / in all contexts, for the specified destination unicast or multicast MAC address to which filtering information of wild card entry is applied.
- broadcast - Displays the wildcard MAC entries created in the switch / in all contexts, for the broadcast MAC address (that is, ff:ff:ff:ff:ff:ff).
- switch <context_name> - Displays the wildcard MAC entries for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show wildcard mac-address 00:11:22:33:00:00
Wild Card Entries:
----------------------------
Mac Address                Ports
-------------------------  ------------------------------
00:11:22:33:00:00       Gi0/2
```

Related Command(s)

- wildcard - Configures the wildcard VLAN entry for a specified MAC address or any MAC address.
- no shutdown vlan - Starts and enables VLAN switching feature in the switch.

shutdown garp

Command Objective This command shuts down the GARP module in the switch on all ports and releases all memories used for the GARP module.

The no form of the command starts and enables the GARP module in the switch on all ports. GMRP and GVRP are enabled explicitly, once the disabled GARP is enabled.

GARP is used to synchronize attribute information between the bridges in the LAN. It allows registering and de-registering attribute values, which are disseminated into the backbone of the GARP participants.

Syntax **shutdown garp**

no shutdown garp

Mode Global Configuration Mode

Default GARP module is started and enabled in the switch on all ports.

Notes:

- GARP can be started, only if VLAN switching feature is started in the switch.
- GARP can be shutdown, only if GVRP and/or GMRP are disabled.
- GARP cannot be started in the switch, if the base bridge mode is configured as transparent bridging.

Example

```
Your Product(config)# shutdown garp
```

Related Command(s)

- `base bridge-mode` - Configures the base mode (either 802.1d transparent bridge mode or 802.1q vlan aware bridge mode) in which the VLAN feature should operate on the switch.
- `set gvrp disable` – Globally disables GVRP feature on all ports of a switch.
- `set port gvrp` - Enables or disables GVRP feature on the specified interface.
- `set gmrp disable` – Globally disables GMRP feature on all ports of a switch.
- `set port gmrp` - Enables or disables GMRP feature on the specified interface.
- `set garp timer` - Configures GARP timers for a port.
- `vlan restricted` - Configures the restricted VLAN registration feature in a port.
- `group restricted` - Configures the restricted group registration feature in a port.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show garp timer` - Displays the GARP timer information of all interfaces available in the switch / all contexts.
- `debug garp` - Enables the tracing of the GARP submodule as per the configured debug levels.

set gvrp

Command Objective This command globally enables or disables GVRP feature on all ports of a switch.

GVRP uses the services of GARP to propagate VLAN registration information to other VLAN aware bridges in a LAN. This information allows GVRP aware devices to dynamically establish and update the information about the existence of the VLANs in a topology. The GVRP registers the created VLANs with GARP and de-registers the deleted VLANs from the GARP.

Syntax **set gvrp { enable | disable }**

Parameter Description

- **enable** - Enables GVRP feature in the switch on all ports and also starts the GARP in the switch if the GARP is disabled.
- **disable** - Disables GVRP feature in the switch on all ports.

Mode Global Configuration Mode

Default enable

Notes:

- GVRP feature can be globally enabled, only if VLAN feature is globally enabled in the switch.
- GVRP feature should be globally disabled before globally disabling the VLAN feature in the switch.
- GVRP feature cannot be enabled in the switch, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.

Example

```
Your Product(config)# set gvrp disable
```

Related Command(s)

- `spanning-tree mode` - Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.
- `set vlan` - Globally enables / disables VLAN feature in the switch (that is the status of the VLAN feature is configured for all ports of the switch).
- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `shutdown garp` - Shuts down the GARP module in the switch on all ports and releases all memories used for the GARP module.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan device info` - Displays the VLAN global information that is applicable to all VLANs created in the switch / all contexts.
- `show gvrp statistics` - Displays GVRP statistics for the specified port.

set port gvrp

Command Objective This command enables or disables GVRP feature on the specified interface.

GVRP uses the services of GARP to propagate VLAN registration information to other VLAN aware bridges in a LAN. This information allows GVRP aware devices to dynamically establish and update the information about the existence of the VLANs in a topology. The GVRP registers the created VLANs with GARP and de-registers the deleted VLANs from the GARP.

Syntax **set port gvrp <interface-type> <interface-id> { enable | disable }**

Parameter Description

- `<interface-type>` - Configures the GVRP feature for the specified type of interface. The interface can be:
  - `qx-ethernet` **–** A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet`**–** A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` **–** A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `port-channel`**–** Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Configures the GVRP feature for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For example: 1 represents port-channel ID.
- `enable` - Enables GVRP feature on the specified interface.
- `disable` - Disables GVRP feature on the specified interface.

Mode Global Configuration Mode

Default enable

Notes:

- The GVRP feature can be configured on the specified interface, only if the GARP module is not shutdown.
- Any GVRP packet received is discarded and no GVRP registrations are propagated from other ports, if GVRP is globally disabled or GVRP is disabled in the interface.

Example

```
Your Product(config)# set disable
port gvrp gigabitethernet 0/1
```

Related Command(s)

- `no shutdown garp` - Starts and enables the GARP module in the switch on all ports.
- `switchport mode` - Configures the mode of operation for a switch port.
- `shutdown garp` - Shuts down the GARP module in the switch on all ports and releases all memories used for the GARP module.
- `show vlan port config` - Displays the VLAN related port specific information for all interfaces available in the switch / all contexts.
- `show gvrp statistics` - Displays GVRP statistics for the specified port.

set port gvrp - enable | disable

Command Objective This command enables or disables GVRP (GARP VLAN Registration Protocol) on the interface.

This command operates similar to that of the command set port gvrp. This feature has been included in adherence to the Industry Standard CLI syntax.

Syntax **set port gvrp { enable | disable } <interface-id>**

Parameter Description

- `enable` - Enables GVRP on the interface
- `disable` - Disables GVRP on the interface
- `<interface-id>` - Configures the GVRP feature for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a Mode slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan and port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

Mode Global Configuration Mode

Default enable

Notes:

- The value enable indicates that GVRP is enabled on the current port, as long as global GVRP status is also enabled for the device
- If port GVRP state is disabled, but global GVRP status is still enabled, then GVRP is disabled on current port. Any received GVRP packets will be discarded and no GVRP registrations will be propagated from other ports

Example `Your Product(config)# set port gvrp disable 0/1`

Related Command(s) `show vlan port config` - Displays the vlan related parameters specific for ports

set gmrp

Command Objective This command globally enables or disables GMRP feature on all ports of a switch.

GMRP uses the services of GARP to propagate multicast information to the bridges in a LAN. This information allows GMRP aware devices to reduce the transmission of multicast traffic to the LANs, which do not have any members of that multicast group. GMRP registers and de-registers the group membership information and group service requirement information with the GARP.

Syntax **set gmrp { enable | disable }**

Parameter Description

- `enable` - Enables GMRP feature in the switch on all ports and also starts the GARP in the switch if the GARP is disabled..
- `disable` - Disables GMRP feature in the switch on all ports.

Mode Global Configuration Mode

Default enable

Notes:

- GMRP feature can be globally enabled, only if VLAN feature is globally enabled in the switch.
- GMRP feature should be globally disabled before globally disabling the VLAN feature in the switch.
- GMRP feature cannot be configured in the switch, if the base bridge mode is set as transparent bridging or the VLAN switching feature is shutdown in the switch.

Example `Your Product(config)# set gmrp disable`

Related Command(s)

- `set vlan` - Globally enables / disables VLAN feature in the switch (that is the status of the VLAN feature is configured for all ports of the switch).
- `base bridge-mode dot1q-vlan` - Configures the VLAN operation mode as VLAN aware bridging.
- `shutdown garp` - Shuts down the GARP module in the switch on all ports and releases all memories used for the GARP module.
- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show vlan device info` - Displays the VLAN global information that is applicable to all VLANs created in the switch / all contexts.

- show gmrp statistics - Displays GMRP statistics for the specified port.

set port gmrp

Command Objective This command enables or disables GMRP feature on the specified interface.

GMRP uses the services of GARP to propagate multicast information to the bridges in a LAN. This information allows GMRP aware devices to reduce the transmission of multicast traffic to the LANs, which do not have any members of that multicast group. GMRP registers and de-registers the group membership information and group service requirement information with the GARP.

Syntax **set port gmrp <interface-type> <interface-id> { enable | disable }**

Parameter Description

- <interface-type> - Configures the GMRP feature for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- <interface-id> - Configures the GMRP feature for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For example: 1 represents port-channel ID.
- enable - Enables GMRP feature on the specified interface.
- disable - Disables GMRP feature on the specified interface.

Mode Global Configuration Mode

Default enable

Notes:

- The GMRP feature can be configured on the specified interface, only if the GARP module is not shutdown.
- Any GMRP packet received is discarded and no GMRP registrations are propagated from other ports, if GMRP is globally disabled or GMRP is disabled inthe interface.

Example

```
Your Product(config)# set disable
port gmrp gigabitethernet 0/1
```

Related Command(s)

- `no shutdown garp` - Starts and enables the GARP module in the switch on all ports.
- `show vlan port config` - Displays the VLAN related port specific information for all interfaces available in the switch / all contexts.
- `show gmrp statistics` - Displays GMRP statistics for the specified port.

set garp timer

Command Objective This command configures GARP timers for a port. GARP uses these timer values to control the transmission of GARP PDUs used in synchronizing attribute information between the switches, and in registering and de-registering of attribute values. The configured GARP timer values are applicable for both GVRP and GMRP application of the GARP module.

Syntax **set garp timer {join | leave | leaveall} <time in milli seconds>**

Parameter Description

- `join <time in milli seconds>` - Configures the time interval (in milli- seconds) till which a GARP participant should wait for its join message to be acknowledged before re-sending the join message. The join message is re- transmitted only once, if the initial message is not acknowledged. This time is started, once the initial join message is sent. The join message is sent by a GARP participant to another GARP participant for registering:
  - Its attributes with other participant
  - Its manually configured attributes
  - Attributes received from a third GARP participant

  This value can be multiple of tens only (that is, as 210, 220, 230 and so on) This value should satisfy the condition: GarpJoinTime > 0 and (2*GarpJoinTime) < GarpLeaveTime.

- `leave <time in milli seconds>` - Configures the time interval (in milli-seconds) till which a GARP participant should wait for any join message before removing attribute details (that is, waiting time for a registrar to move from empty state (MT) to leave state (LV)). This time is started, once a leave message is sent to de-register the attribute details. The leave messages are sent from a GARP participant to another participant, when:
  - Its attributes should be de-registered
  - Its attributes are manually de-registered
  - It receives leave messages from a third GARP participant

  This value can be multiple of tens only (that is, as 610, 620, 630 and so on). The leave time should be greater than or two times as that of the GarpJoinTime. That is, the maximum value of the leave time cannot be more than two times of the join time. For example, if you configure join time as 500 milliseconds, then the leave time value can be from 510 milliseconds to 1000 milliseconds only.

- `leaveall <time in milli seconds>` - Configures the time interval (in milli-seconds) till which the details of the registered attributes are maintained. The attribute details should be re- registered after this time interval. A leaveall message is sent from a GARP participant to other GARP participants, after this time interval. This time is started, once a GARP participant starts/once re-registration is done. The leaveall messages are sent from a GARP participant to other participants for:
  - De-registering all registered attributes
  - Re-registering all attributes with each of the participants

  This value can be multiple of tens only (that is, as 10010, 10020 and so on). The leaveall time should be greater than 0 and greater than GarpLeaveTime.

Mode Interface Configuration Mode (Physical)

Default

- join - 200
- leave - 600
- leaveall - 10000

Notes:

- The GARP timers cannot be set as zero.
- The GARP timers can be configured, only if the GARP module is not shutdown.

Example

```
Your Product(config-if)# set garp timer join 250
```

Related Command(s)

- `no shutdown garp` - Starts and enables the GARP module in the switch on all ports.
- `show garp timer` - Displays the GARP timer information of all interfaces available in the switch / all contexts.

vlan restricted

Command Objective This command configures t feature configures the restricted VLAN registration feature in a port. This feature configures the dynamic registration of VLAN.

Syntax **vlan restricted {enable | disable}**

Parameter Description

- `enable` - Enables restricted VLAN registration feature in the port. The creation or modification of a dynamic VLAN entry is permitted only for VLANs for which static VLAN registration entries exist.
- `disable` - Disables restricted VLAN registration feature in the port. The creation or modification of

a dynamic VLAN entry is permitted only for all VLANs.

Mode Interface Configuration Mode (Physical)

Default disable

Note: The restricted VLAN registration feature can be configured in the port, only if the GARP module is started and enabled in the switch.

Example

```
Your Product(config-if)# vlan restricted enable
```

Related Command(s)

- `no shutdown garp` - Starts and enables the GARP module in the switch on all ports.
- `show vlan port config` - Displays the VLAN related port specific information for all interfaces available in the switch / all contexts.

group restricted

Command Objective This command configures the restricted group registration feature in a port. This feature enables you to restrict the multicast groups learnt through GMRP learning.

Syntax **group restricted {enable | disable }**

Parameter Description

- `enable` - Enables restricted group registration feature in the port. The multicast group attribute / service requirement attribute is learnt dynamically from the GMRP frame only if the specific attribute is statically configured in the switch.
- `disable` - Disables restricted group registration feature in the port. The GMRP packets are processed normally and the multicast group attribute/service requirement attribute are learnt dynamically even if they are not statically configured in the switch.

Mode Interface Configuration Mode (Physical)

Default disable

Note: The restricted group registration feature can be configured in the port, only if the GARP module is started and enabled in the switch.

Example

```
Your Product(config-if)# group restricted enable
```

Related Command(s)

- `no shutdown garp` - Starts and enables the GARP module in the switch on all ports.
- `show vlan port config` - Displays the VLAN related port specific information for all interfaces available in the switch / all contexts.

debug garp

Command Objective This command enables the tracing of the GARP sub module as per the configured debug levels. The trace statements are generated for the configured trace levels.

The no form of the command disables the tracing of the GARP sub module as per the configured debug levels. The trace statements are not generated for the configured trace levels.

This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

Syntax **debug garp { global | [{protocol | gmrp | gvrp | redundancy} [initshut] [mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all]] [switch <context_name>] }**

no debug garp { global | [{protocol | gmrp | garp | redundancy} [initshut] [mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all]] [switch <context_name>] }

Parameter Description

- `global` - Generates debug statements for all kinds of traces.
- protocol - Sets the submodule as GARP module, for which the tracing is to be done as per the configured debug levels.
- `gmrp` - Sets the submodule as GMRP module, for which the tracing is to be done as per the configured debug levels.
- `gvrp` - Sets the submodule as GVRP module, for which the tracing is to be done as per the configured debug levels.
- `redundancy` - Sets the submodule as GARP redundancy module, for which the tracing is to be done as per the configured debug levels.
- `initshut` - Generates debug statements for init and shutdown traces. This trace is generated on failed initialization and shutting down of GARP related entries.
- `mgmt` - Generates debug statements for management traces. This trace is generated during failure in configuration of any of the GARP features.
- `data` - Generates debug statements for data path traces. This trace is generated during failure in packet processing.
- `ctpl` - Generates debug statements for control path traces. This trace is generated during failure in modification or retrieving of GARP entries.
- `dump` - Generates debug statements for packet dump traces. This trace is currently not used in GARP module.
- `os` - Generates debug statements for OS resource related traces. This trace is generated during failure in message queues.
- `failall` - Generates debug statements for all kind of failure traces.
- `buffer` - Generates debug statements for GARP buffer related traces. This trace is currently not used in GARP module.
- `all` - Generates debug statements for all kinds of traces.

- `switch <context_name>` - Configures the tracing of the GARP submodule for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged Exec Mode

Default Tracing of the GARP sub module is disabled.

Note: The GARP sub module tracing can be configured in the switch, only if the GARP module is started and enabled in the switch on all ports.

Example `Your Product# debug garp gvrp all`

Related Command(s)

- `no shutdown garp` - Starts and enables the GARP module in the switch on all ports.
- `show debugging` - Displays state of each debugging option.

show garp timer

Command Objective This command displays the GARP timer information of all interfaces available in the switch / all contexts. The information contain the interface type, interface ID, GARP join time, GARP leave time and GARP leave all time.

Syntax **show garp timer [{ port <interface-type> <interface-id> | switch <context_name>}]**

Parameter Description

- port - Displays the GARP timer information of the specified interface. The details to be provided are:
  - `<interface-type>` - Sets the type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
  - `<interface-id>` - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID isprovided, for interface type port-channel.
- `switch <context_name>` - Displays the GARP timer information of all interfaces, for the specified context. This value represents unique name of the switch context. This value is a string with the

maximum size as 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Note: This command can be executed in the switch, only if the GARP module is not shutdown and VLAN switching feature is started and enabled in the switch.

Example

```
Your Product# show garp timer port gigabitethernet 0/1
Garp Port Timer Info (in milli seconds)
--------------------------------------------------------------
Port                     Join-time       Leave-time    Leave-all-time
-----                    --------------------    --------------
Gi0/1                    200             600           10000
```

Related Command(s)

- set garp timer - Configures GARP timers for a port.
- no shutdown garp - Starts and enables the GARP module in the switch on all ports.
- no shutdown vlan - Starts and enables VLAN switching feature in the switch.

switchport unicast-mac learning

Command Objective This command enables / disables unicast-MAC learning for the port.

Syntax **switchport unicast-mac learning { enable | disable }**

Parameter Description

- enable - Enables unicast-MAC learning for the port.When Mac Learning is enabled, unicast mac entries will be learnt on this port. Configuration of this object will not get affected by the Global MacLearning Status
- disable - Disables unicast-MAC learning for the port. When Unicast Mac Learning is disabled, no unicast mac entry will be learnt on this port.

Mode Interface Configuration Mode (Physical / Port channel)

Default enable

Example `Your Product(config-if)# switchport unicast-mac learning enable`

Related Command(s) show [provider-bridge] port config - Displays Service VLAN port information

private-vlan

Command Objective This command configures the private vlan type for the vlan to provide layer2 isolation between the ports within the same broadcast domain.

The no form of the command removes the pvlan type for the vlan.

Syntax **private-vlan { primary | isolated | community }**

no private-vlan

Parameter Description

- `primary` - Encompasses the entire private VLAN domain. It is a part of each subdomain and provides the Layer 3 gateway out of the VLAN. A private VLAN domain has only one primary VLAN. Every port in a private VLAN domain is a member of the primary VLAN
- `isolated` - Configures an isolated VLAN which is a secondary VLAN in which all hosts connected to its ports are isolated at Layer 2. An isolated port has complete Layer 2 separation from the other ports within the same PVLAN, but not from the promiscuous ports. Traffic from isolated port is forwarded only to promiscuous ports.
- `community` - Configures a community VLAN which is a secondary VLAN that is associated to a group of ports that connect to a certain "community" of end devices with mutual trust relationships. Community ports communicate among themselves and with their promiscuous ports. These interfaces are separated at Layer 2 from all other interfaces in other communities or isolated ports within their PVLAN.

Mode Config-VLAN Mode

Note: This command executes only if the VLAN is created without IVR interface.

Example

```
Your Product(config-vlan)# private-vlan primary
```

Related Command(s) `show vlan private-vlan` - Displays the private-VLAN information for the switch

private-vlan association

Command Objective This command maps the list of vlans to a primary vlan and associates a specified secondary VLAN with the primary VLAN to function as a PVLAN domain in the running configuration.

The no form of the command removes the secondary vlan from the primary vlan association.

Syntax **private-vlan association [{add|remove}]<secondary_Vlan_list>**

no private-vlan association

Parameter Description

- `add` - Adds the given list of vlans to the existing secondary vlan list
- `remove` - Removes the given list of vlans from the existing secondary vlan list
- `<secondary_Vlan_list>` - Replaces the existing vlans with the given list of secondary vlans, if add and remove is not given. This value ranges between 1 and 4094. Use comma as a separator without space while configuring list of vlans. Example: 502,4094.

Mode Config-VLAN Mode

Note: This command executes only when primary and secondary vlan are created.

Example Your Product(config-vlan)# private-vlan association add 303,1000

Related Command(s)

- `private-vlan` - Configures the private vlan type for the vlan to provide layer 2 isolation between the ports
- `show vlan private-vlan` - Displays the private-VLAN information for the switch

switchport private-vlan host-association

Command Objective This command configures the association between the primary and secondary vlan id to host port.

The no form of the command deletes the primary and secondary vlan id association from host.

Syntax **switchport private-vlan host-association <primary-vlanId(1-4094)> <secondary-vlanId(1-4094)>**

no switchport private-vlan host-association

Parameter Description

- `<primary-vlanId(1-4094)>` - Configures a unique value that represents the specific Primary VLAN to which the switch port has to be associated. This value ranges between 1 and 4094
- `<secondary-vlanId(1-4094)>` - Configures a unique value that represents the specific secondary to which the switch port has to be associated. This value ranges between 1 and 4094.

Mode Interface configuration mode(Physical / Port channel)

Note: This command executes only when primary and secondary vlan are created and configured

Example

```
Your Product(config-if)# switchport private-vlan host- association 35 55
```

Related Command(s)

- `private-vlan` - Configures the private vlan type for the vlan to provide layer 2 isolation between the ports
- `show vlan private-vlan` - Displays the private-VLAN information for the switch

switchport private-vlan mapping

Command Objective This command maps the Private VLAN promiscuous port to the primary VLAN and to the selected secondary VLANs.

The no form of the command unmaps the primary and secondary vlan association for this promiscuous port.

Syntax **switchport private-vlan mapping <primary_vlan_id(1-4094)> [{add | remove}] [<secondary_vlan_list>]**

no switchport private-vlan mapping

Parameter Description

- `<primary_vlan_id(1-4094)>` - Configures a unique value that represents the specific Primary VLAN to which the promiscuous switchport is to be mapped.This value ranges between 1 and 4094.
- `add` - Maps the list of secondary vlan id to this primary VLAN ID and switch port.
- `remove` - Unmaps the given list of primary VLAN ID from the existing secondary vlan list.
- `<secondary_vlan_list>` - Configures the list of secondary vlan id to which the promiscuous port is associated in the Private VLAN domain. This value ranges between 1 and 4094.Use comma as a separator without space while configuring list of vlans. Example: 502,4094.

Mode Interface configuration mode (Physical / Port channel)

Example Your Product(config-if)# switchport private-vlan mapping 34 add 35,36

Related Command(s) `show vlan private-vlan` - Displays the private-VLAN information for the switch

show vlan private-vlan

Command Objective This command displays the private-VLAN information for the switch.

Syntax **show vlan private-vlan [{primary | isolated | community}] [switch <context_name>]**

Parameter Description

- `primary` - Displays the private VLAN information for primary primary, VLAN.
- `isolated` - Displays the private VLAN information for isolated VLAN.
- `community` - Displays the private VLAN information for community VLAN.
- `switch <context_name>` - Displays private vlan information for the specified context. This value represents unique name of the switch context. This value is a string of maximum size 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show vlan private-vlan
Switch default switch default
VlanId                    Type         Primary VlanId            Ports
```

```
2                        isolated                10
10                       primary                 -
Your Product # show vlan private-vlan isolated-------          --------
Switch default
switch default
VlanId                Type          Primary VlanId          Ports
------------          ----------    ----------------------  --------
2                     isolated      10
```

Related Command(s)

- `private-vlan` - Configures the private vlan type for the vlan to provide layer 2 isolation between the ports.
- `private-vlan association` - Maps the list of vlans to a primary vlan and associates a specified secondary VLAN with the primary VLAN to function as a PVLAN domain in the running configuration.
- `switchport private-vlan host-association` – Configures the association between the primary and secondary vlan id to host port.
- `switchport private-vlan mapping` - Maps the Private VLAN promiscuous port to the primary VLAN and to the selected secondary VLANs.

set filtering-utility-criteria

Command Objective This command sets the filtering utility criteria to be applied on all ports.

Syntax **set filtering-utility-criteria { enable | disable }**

Parameter Description

- `enable` - Applies the filtering utiltiy criteria configured on the port.It can be default or enhanced.

  If enhanced filtering utility criteria is selected on a port, then learning of source mac from a received packet on that port will be done if the following are satisfied:

  - If at least one VLAN that uses the FID includes the reception Port and at least one other Port with a Port State of Learning or Forwarding in its member set, and:
    - The operPointToPointMAC parameter is false for the reception Port;

      or

  - Ingress to the VLAN is permitted through a third Port. The third port can, but is not required to, be in the member set.
- `disable` - Sets default filtering utility criteria to be applied on all ports. If default filtering utility Criteria is selected on a port, then learning of source mac from a received packet on that port will be done only if there is atleast on member port in that vlan.

Mode Global Configuration Mode / Switch Configuration Mode

Default enable

Example Your Product(config)# set filtering-utility-criteria enable

Related Command(s) `show vlan device info` - Displays the VLAN global information that is applicable to all VLANs created in the switch / all contexts

set sw-stats

Command Objective This command sets the software statistics collection globally in the switch.

Syntax **set sw-stats { enable | disable }**

Parameter Description

- `enable` - Enables Software statistics collection globally in the switch and the statistics will be stored in the software. This value can be set only if data switching is done by the software.
- `disable` - Disables Software statistics collection globally in the switch. The statistics collection will be done by the hardware and will not be stored in software

Mode Global Configuration Mode

Default If data switching is done by software, then the default value is enabled else by default statistics collection by the software is disabled.

Example Your Product(config)# set sw-stats enable

Related Command(s) `show vlan statistics` - Displays the unicast / broadcast statistics details of all active VLANs and VLANs (that are not active) for which the port details are configured.

set vlan counter

Command Objective This command enables or disables the statistics collection for the specified VLAN.

Syntax **set vlan counter { enable | disable }**

Parameter Description

- `enable` - Enables statistics collection for the VLAN.
- `disable` - Disables statistics collection for the VLAN.

Mode Config VLAN Mode

Default disable

Note: This command executes only if the VLAN is set to active or if the member ports are associated with the VLAN.

Example

```
Your Product(config)# set vlan counter enable
```

Related Command(s)

- `vlan active` - Activates a VLAN in the switch.
- `ports` - Configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN.
- `show vlan statistics` - Displays the unicast / broadcast statistics details of all active VLANs and VLANs (that are not active) for which the port details are configured.

clear mac-address-table dynamic

Command Objective This command clears the dynamically learnt MAC Addresses.

Syntax **clear mac-address-table dynamic [interface {port-channel <port-channel-id (1-65535)> | <interface-type> <interface- id>}] [vlan <vlan_vfi_id>]**

Parameter Description

- `port-channel <port-channel-id (1-65535)>` - Clears the FDB entries for the specified port channel interface. Port-Channel are logical interfaces that represents an aggregator which contains several ports aggregated together. This value ranges between 1 and 65535
- `<interface-type>` - Clears the FDB entries for the specified type of interface. The interface can be:
  - `qx-ethern`et **–** A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` **–** A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - `extreme-ethernet` **–** A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Clears the FDB entries for the interface identifier of the specified type of interface. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel is provided, for interface type port-channel.
- `vlan <vlan-id/vfi-id>` - Clears the FDB entries for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - <vlan **–**id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

  Notes:

  1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
  2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
  3. The theoretical maximum for the maximum number of VFI is 65535 but the actual

number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

Mode Global Configuration Mode/ Switch Configuration Mode

Example

```
Your Product(config)# clear mac-address-table dynamic
```

Related Command(s)

- `show mac-address-table static unicast` - Displays the statically configured unicast address from the MAC address table.
- `show mac-address-table static multicast` - Displays the statically configured multicast entries.

debug vlan global

Command Objective This command enables tracing in VLAN sub module and generates debug statements for global traces.

The no form of the disables tracing of the VLAN sub module .

Syntax **debug vlan global**

no debug vlan global

Mode Privilege Exec Mode

Default Tracing of the VLAN sub module is disabled.

Note: The VLAN sub module tracing related configuration takes effect in the switch, only if the VLAN switching feature is started and enabled in the switch.

Example Your Product# debug vlan global

Related Command (s)

- `no shutdown vlan` - Starts and enables VLAN switching feature in the switch.
- `show debugging` - Displays state of each debugging option.

show gmrp statistics

Command Objective This command displays GMRP statistics for the specified port.

Syntax **show gmrp statistics [{ port <interface-type> <interface- id> }]**

Parameter Description

- `<interface-type>` - Displays GMRP statistics for the specified type of interface. The interface can be:
    - `qx-ethernet` **–** A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` **–** A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - `extreme-ethernet` **–** A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `port-channel` **–** Logical interface that represents an aggregator which contains several ports aggregated together.
    - `pw` - Pseudowire (PW) is a emulation of a point-to-point connection over a packet-switching network (PSN). This value ranges between 1 and 65535. Maximum number of PseudoWire interfaces supported in the system is 100. This interface type is not supported.
    - `ac` - Attachment Circuit (AC) is a physical or virtual circuit attaching a Customer Edge to a Provider Edge port. This value ranges between 1 and 65535. This interface type is not supported.
- `<interface-id>` - Displays GMRP statistics for the interface id of the specified type of interface. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel.

Mode Privileged EXEC Mode

Example Your Product# show gmrp statistics gi 0/1

Related Command(s)

- `set gmrp`– Globally enables or disables GMRP feature on all ports of a switch
- `set port gmrp`- Enables or disables GMRP feature on the specified interface

show gvrp statistics

Command Objective This command displays GVRP statistics in the system or for the specified port.

Syntax **show gvrp id> }] statistics [{ port <interface-type> <interface-**

Parameter Description

- `<interface-type>` - Displays GVRP statistics for the specified type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.

  - gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
  - pw - Pseudowire (PW) is a emulation of a point-to-point connection over a packet-switching network (PSN). This value ranges between 1 and 65535. Maximum number of PseudoWire interfaces supported in the system is 100. This interface type is not supported.
  - ac - Attachment Circuit (AC) is a physical or virtual circuit attaching a Customer Edge to a Provider Edge port. This value ranges between 1 and 65535. This interface type is not supported.
- <interface-id> - Displays GVRP statistics for the interface id of the specified type of interface. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel.

Mode Privileged EXEC Mode

Example

```
Your Product# show gvrp statistics port gi 0/1
GVRP Statistics for Port 1
------------------------------------------------------------
Total valid              GVRP     Packets Received: 0
Join Emptys                0
Join In                    0
Leave In                   0
Leave All                  0

Leave Empty                0
Empty                      0
Total valid GVRP Packets Transmitted: 0
Join Emptys                0
Join In                    0
Leave In                   0
Leave All                  0
Leave Empty                0
Empty                      0
```

Related Command(s)

- set gvrp– Globally enables or disables GVRP feature on all ports of a switch
- set port gvrp- Enables or disables GVRP feature on the specified interface

21 VRRP

VRRP (Virtual Router Redundancy Protocol) is an election protocol that dynamically assigns responsibility for one or more virtual router(s) to the VRRP routers(s) on a LAN, allowing several routers on a multi- access link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP setup, one router is elected as the master router with the other routers acting as backups in case of the failure of the master router. VRRP is designed to eliminate the single point of failure inherent in the static default routed environment

The list of CLI commands for the configuration of VRRP is as follows:

- router vrrp
- interface – VRRP
- vrrp - ipv4 address
- vrrp – ip address
- vrrp group shutdown
- vrrp – priority
- vrrp – preempt
- vrrp - text-authentication
- vrrp - authentication text
- vrrp – interval
- vrrp - timers advertise
- show vrrp
- show vrrp interface
- auth-deprecate
- debug ip vrrp

router vrrp

Command Objective This command enables VRRP globally in the router and enters into the VRRP Router Configuration Mode, which allows the user to execute all the commands which supports this mode.

The no form of the command disables VRRP in the router.

Syntax **router vrrp**

no router vrrp

Mode Global Configuration Mode

Example

```
Your Product(config)# router vrrp
Your Product (config-vrrp)#
```

Related Command(s)

- `interface – VRRP` – Enables VRRP in the specified interface.
- `vrrp -ipv4 address` - Sets the associated IP addresses for the virtual router.
- `show vrrp interface` - vrid – Displays the VRRP status information.
- `vrrp group shutdown` – Shuts down all VRRP groups.

interface – VRRP

Command Objective This command enables VRRP for the specified interface and enters into the VRRP Interface Configuration Mode, which allows the user to execute all the commands which supports this mode.

The no form disables VRRP for the specified interface.

Syntax **interface { vlan <vlan-id/vfi-id> | <interface-type> <interface-id> | <IP-interface-type> <IP-interface-number>}**

no interface { Vlan <vlan-id/vfi-id> | <interface-type> <interface-id> | <IP-interface-type> <IP-interface-number>}

Parameter Description

- vlan <vlan-id/vfi-id> - Enables VRRP for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

    Notes:

    1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
    2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
    3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- <interface-type> - Enables VRRP for the specified type of interface. The interface can be:
  - qx-ethernet – A version of Ethernet that support-s data transfer upto 40 Gigabits per

second. This Ethernet supports only full duplex links.

  - gigabitethernet **–** A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet **–** A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.

- <interface-id> - Enables VRRP for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, For example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For example: 1 represents port-channel ID.
- <IP-interface-type> - Enables VRRP in the specified L3 Psuedo wire interface in the system.
- <IP-interface-number> - EnablesVRRP for the specified interface identifier. This is a unique value that represents the specific interface . This value ranges between 1 and 65535 for Psuedowire interface.

Note: Maximum number of PseudoWire interfaces supported in the system is 100.

Mode VRRP Router Configuration Mode

Example

```
Your Product(config-vrrp)# interface vlan 3
Your Product(config-vrrp-if)#
Your Product (config-vrrp)# interface gigabitethernet 0/1
Your Product (config-vrrp-if)#
```

Related Command(s)

- `router vrrp` – Enables VRRP in the router.
- `show vrrp interface - vrid` – Displays the VRRP status information.
- show vrrp interface - Displays the VRRP status information for all VR-ids created on that interface.

vrrp - ipv4 address

Command Objective This command sets the associated IP addresses for the virtual router. On executing this command, the VRRP module starts the transition from ‘Initial’ state to either ‘Backup’ state or ‘Master’ state as per the election process on the specific interface.

The no form of the command deletes the associated IP addresses for the virtual router.

Syntax **vrrp <vrid(1-255)> ipv4 <ip_addr > [secondary]**

no vrrp <vrid(1-255)> ipv4[<ip_addr>[secondary]]

Parameter Description

- `<vrid(1-255)>` - Configures virtual router identifier(VRID)which is a number along with an interface to uniquely identify a virtual router on a given VRRP router. This value ranges between 1 and 255.
- `ipv4 <ip_addr >` - Configures an IPv4 address to be assigned to the VRID.
- `secondary` - Configures the secondary IP address for the specified virtual router.

Mode VRRP Interface Configuration Mode

Note: This command executes only if the associated primary IP address for the virtual router is set.

Example

```
Your Product(config-vrrp-if)# vrrp 3 ipv4 10.0.0.1
```

Related Command(s)

- `router vrrp` – Enables VRRP in the router.
- ip address - Sets an IP address for an interface.
- vrrp – preempt - Enables the pre-emption of state change from either Backup to Master or vice versa based on the election process.
- vrrp - text-authentication / vrrp - authentication text - Sets the authentication type for the virtual router to simple password.
- vrrp - interval / vrrp - timers advertise - Sets the advertisement timer for a virtual router.
- show vrrp interface - vrid – Displays the VRRP status information.
- show vrrp interface - Displays the VRRP status information.

vrrp – ip address

Command Objective This command sets the associated IP addresses for the virtual router. On executing this command the VRRP module starts the transition from 'Initial' state to either 'Backup' state or 'Master' state as per the election process on the specific interface.

Note: This command is a complete standardized implementation of the existing command and operates similar to that of the command vrrp - ipv4 address.

Syntax **vrrp <vrid(1-255)> ip <ip_addr> [secondary]**

Parameter Description

- `<vrid(1-255)>` - Configures virtual router identifier (VRID) which is a number along with an interface to uniquely identify a virtual router on a given VRRP router. This value ranges between 1 and 255.
- `ip <ip_addr >` - Configures a IPv4 addresses to be assigned to the VRID.
- `secondary` - Configures the secondary IP addresses for the specified virtual router.

Mode VRRP Interface Configuration Mode

Note: This command executes only if the associated primary IP addresses for the virtual router is set.

Example `Your product(config-vrrp-if)# vrrp 3 ip 10.0.0.1`

Related Command(s)

- `router vrrp` – Enables VRRP in the router.
- `ip address` - Sets an IP address for an interface.
- `vrrp – preempt` - Enables the pre-emption of state change from either Backup to Master or vice versa based on the election process.
- `vrrp – text-authentication / vrrp – authentication text` - Sets the authentication type for the virtual router to simple password
- `vrrp – interval / vrrp – timers advertise` - Sets the advertisement timer for a virtual router.
- `show vrrp interface – vrid` – Displays the VRRP status information.
- `show vrrp interface` – Displays the VRRP status information.

vrrp group shutdown

Command Objective This command shuts down all VRRP groups.

Note: This command is a complete standardized implementation of the existing command and operates similar to that of the command vrrp - ipv4 address, except that all the associated IP address of the virtual router will be deleted.

Syntax **vrrp group shutdown**

Mode VRRP Interface Configuration Mode

Note: This command executes only if the associated primary IP addresses for the virtual router is set.

Example `Your Product(config-vrrp-if)# vrrp group shutdown`

Related Command(s)

- router vrrp – Enables VRRP in the router.
- show vrrp interface - vrid – Displays the VRRP status information.
- show vrrp interface - Displays the VRRP status information.

vrrp – priority

Command Objective This command sets the priority for the virtual router.

The no form of the command sets the priority for the virtual router to its default value.

Syntax **vrrp <vrid(1-255)> priority <priority(1-254)>**

no vrrp <vrid(1-255)> priority

Parameter Description

- `<vrid(1-255)>` - Configures a virtual router ID for which the priority is to be set. This value ranges between 1 and 255.
- `<priority(1-254)>` - Sets the priority which is used for the virtual router master election process. Higher values imply a higher priority. A priority of 255 is used for the router that owns the associated IP address(es).

Mode VRRP Interface Configuration Mode

Note: This command executes only if the associated primary IP addresses for the virtual router is set.

Default priority -100

Example

```
Your Product(config-vrrp-if)# vrrp 3 priority 7
```

Related Command(s)

- `ip address` - Configures IP address for an interface.
- `router vrrp` – Enables VRRP in the router.
- `interface – VRRP` – Enables VRRP in the specified interface.
- `vrrp – ipv4 address` - Sets the associated primary IP addresses for the virtual router.
- `show vrrp interface – vrid` – Displays the VRRP status information.

vrrp – preempt

Command Objective This command enables the pre-emption of state change from either Backup to Master or vice versa based on the election process.

The no form of the command disables the preempt mode.

Syntax **vrrp <vrid(1-255)> preempt [delay minimum <value(0-30)>]**

no vrrp <vrid(1-255)> preempt

Parameter Description

- `vrid<vrid(1-255)>` - Configures a virtual router ID for which the preempt state change is to be enabled. The value ranges between 1 and 255.
- `delay minimum <value(0-30)` - Sets the number of seconds that the router will delay before issuing an advertisement claiming master ownership. This value ranges between 0 and 30.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode VRRP Interface Configuration Mode

Default

- delay minimum - 0
- Pre-emption is enabled.

Note: This command executes only if the associated primary IP addresses for the virtual router is set.

Example

```
Your product(config-vrrp-if)# vrrp 3 preempt
```

Related Command(s)

- `ip address` - Configures IP address for an interface.
- `router vrrp` – Enables VRRP in the router
- `interface - VRRP` – Enables VRRP in the specified interface.
- `vrrp - ipv4 address` - Sets the associated primary IP addresses for the virtual router
- `show vrrp interface - vrid` – Displays the VRRP status information
- `show vrrp interface` - Displays the VRRP status information

vrrp - text-authentication

Command Objective This command sets the authentication type for the virtual router to simple password.

The no form of the command sets the authentication type for the virtual router to none

Syntax **vrrp <vrid(1-255)> text-authentication <password>**

no vrrp <vrid(1-255)> text-authentication

Parameter Description

- `vrrp <vrid(1-255)>` - Configures a virtual router ID for which the authentication type is to be set. This value ranges between 1 and 255.
- `<password>` - Sets the authentication password which is used to validate the incoming VRRP packets. The maximum value of this string is 8.

Mode VRRP Interface Configuration Mode

Note: This command executes only if

- The associated IP addresses for the virtual router is set
- Auth depreciate is disabled.

Example

```
Your Product(config-vrrp-if)# vrrp 3 text-authentication pwd
```

Related Command(s)

- ip address - Configures IP address for an interface.
- router vrrp – Enables VRRP in the router.
- interface - VRRP – Enables VRRP in the specified interface.
- vrrp - ipv4 address - Sets the associated IP addresses for the virtual router.
- auth-deprecate – Disables the auth depreciate.
- show vrrp interface - vrid – Displays the VRRP status information.

vrrp - authentication text

Command Objective This command sets the authentication type for the virtual router to simple password.

Note: This command is a complete standardized implementation of the existing command and operates similar to that of the command vrrp - text-authentication.

This feature has been included in adherence to the Industry Standard CLI syntax

Syntax **vrrp <vrid(1-255)> authentication text <password>**

Parameter Description

- vrrp <vrid(1-255)> - Configures a virtual router ID for which the authentication type is to be set. This value ranges between 1 and 255.
- <password> - Sets the authentication password which is used to validate the incoming VRRP packets. The maximum value of this string is 8.

Mode VRRP Interface Configuration Mode

Note: This command executes only if

- associated IP addresses for the virtual router is set.
- Auth depreciate is disabled.

Example

```
Your Product(config-vrrp-if)# vrrp 3 authentication text abcdefgh
```

Related Command(s)

- ip address - Configures IP address for an interface.
- router vrrp – Enables VRRP in the router.
- interface – VRRP – Enables VRRP in the specified interface.
- vrrp - ipv4 address - Sets the associated IP addresses for the virtual router.
- auth-deprecate – Disables the auth depreciate.
- show vrrp interface - vrid – Displays the VRRP status information.

vrrp – interval

Command Objective This command sets the advertisement timer for a virtual router and sends only the master router advertisements.

The no form of the command sets the advertisement timer for a virtual router to default value.

Syntax **vrrp <vrid(1-255)> timer [msec] <interval(1-255)secs>**

no vrrp <vrid(1-255)> timer

Parameter Description

- vrrp <vrid(1-255)> - Configures the Virtual Router ID for which the advertisement timer is to be set. This value ranges between 1 and 255.
- msec - Sets the of advertisement time in milliseconds.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- timer <interval(1-255)secs> - Configures the time interval between successive advertisement messages in seconds. On expiry of the advertise timer, the Master sends advertisement packets to the Backup. This value ranges between 1 and 255 in seconds.

Mode VRRP Interface Configuration Mode

Default 1 second

Note: This command executes only if the associated primary IP addresses for the virtual router is set.

Example

```
Your product(config-vrrp-if)# vrrp 4 timer 6
```

Related Command(s)

- `ip address` - Configures IP address for an interface.
- `router vrrp` – Enables VRRP in the router
- `interface - VRRP` – Enables VRRP in the specified interface.
- `vrrp - ipv4 address` - Sets the associated primary IP addresses for the virtual router
- `show vrrp interface - vrid` – Displays the VRRP status information

vrrp - timers advertise

Command Objective This command sets the advertisement timer for a virtual router and sends only the master router advertisements.

Note: This command is a complete standardized implementation of the existing command and operates similar to that of the command vrrp - interval

This feature has been included in adherence to the Industry Standard CLI syntax.

Syntax **vrrp <vrid(1-255)> timers 255)secs> advertise [msec] <interval(1-**

Parameter Description

- `vrrp <vrid(1-255)>` - Configures the Virtual Router ID for which the
- `msec` - Sets the of advertisement time in milliseconds.

Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- `<interval(1-255)secs>` - Configures the time interval between successive advertisement messages in seconds. On expiry of the advertise timer, the Master sends advertisement packets to the Backup. This value ranges between 1 and 255 in seconds.

Mode VRRP Interface Configuration Mode

Default 1 second

Note: This command executes only if the associated IP addresses for the virtual router is set

Example

```
Your product(config-vrrp-if)# vrrp 3 timers advertise 100
```

Related Command(s)

- `ip address` - Configures IP address for an interface.
- `router vrrp` – Enables VRRP in the router.
- `interface` – VRRP – Enables VRRP in the specified interface.
- `vrrp - ipv4 address` - Sets the associated IP addresses for the virtual router.
- `show vrrp interface - vrid` – Displays the VRRP status information.

show vrrp

Command Objective This command displays the VRRP status information. for the specified VR ID .

Syntax **show vrrp [interface { vlan <VlanId/vfi-id> | <interface- type> <interface-id> | <IP-interface-type> <IP-interface- number> } <VrId(1-255)>] [{brief|detail |statistics}]**

Parameter Description

- `vlan <VlanId/vfi-id>`- Displays the VRRP status information for the specified VLAN/ VFI ID. This value ranges between 1 and 65535.
  - `<vlan -id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - `<vfi-id>.` - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type

is not supported.

Notes:

1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- `<interface-type>` - Displays the VRRP status information for the specified type of interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Displays the VRRP status information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel.For example: 0/1 represents that the slot number is 0 and port number is 1.
- `<IP-interface-type>` - Displays VRRP related configuration for the specified L3 Psuedo wire interface in the system.
- `<IP-interface-number>` - Displays VRRP related configuration for the specified interface identifier. This is a unique value that represents the specific interface . This value ranges between 1 and 65535 for Psuedowire interface. This interface is not supported.

  Notes: Maximum number of PseudoWire interfaces supported in the system is 100.

- `<VrId(1-255)>` - Displays the VRID which is a number along with an interface to uniquely identify a virtual router on a given VRRP router.
- `brief` - Displays the brief VRRP status information.
- `detail` - Displays the detailed VRRP status information.
- `statistics` - Displays the statistical information for the VRRP.

Mode Privileged EXEC Mode

Example

```
Your Product# show vrrp interface vlan 2 detail
vlan2 - vrID 1
---------------- State is Master
Virtual IP address is 12.0.0.2
Virtual MAC address is 00:00:5e:00:01:01
Master router is 12.0.0.2
Associated IpAddresses :
---------------------------------------------
12.0.0.2
Advertise time is 1 secs
Current priority is 100
Configured priority is 100, may preempt vlan2 - vrID 2
---------------- State is Master
Virtual IP address is 12.0.0.1
Virtual MAC address is 00:00:5e:00:01:02
Master router is 12.0.0.1
Associated IpAddresses :
---------------------------------------------
12.0.0.1
Advertise time is 1 secs
Current priority is 255
Configured priority is 255, may preempt
Your Product# show vrrp interface vlan 2 brief
P indicates configured to preempt
Interface               vrID     Priority      P      State         Master        VRouter
                                                                    Addr          Addr
------------------      -------  ------------  -      ---------     ------------  ------------
vlan2                   1        100           P      Master        local         12.0.0.2
vlan2                   2        255           P      Master        local         12.0.0.1
Your Product# show vrrp interface vlan 2 statistics
vlan2 - vrID 1
------------------------------
Transitions to Master           : 2
Advertisements Received         : 0
Advertise Internal Errors       : 0
Authentication Failures         : 0
TTL Errors                      : 0
Zero  Priority  Packets  Received  :  1
Zero Priority Packets Sent : 0 Invalid
Type Packets Received : 0 Address List
Errors                          :  0
Invalid   Authentication   Type   :   0
Authentication Type Mismatch     :  0
Packet Length Errors            : 0 vlan2 - vrID 2
------------------------------
Transitions to Master           : 1
Advertisements Received         : 0
Advertise Internal Errors       : 0
Authentication Failures         : 0
TTL Errors                      : 0
Zero Priority Packets Received    : 0
Zero Priority Packets Sent        : 0
Invalid Type Packets Received     : 0
Address List Errors               : 0
```

```
Invalid Authentication Type       : 0
Authentication Type Mismatch      : 0
Packet Length Errors              : 0
Your Product# show vrrp interface vlan 2
P indicates configured to preempt
Interface               vrID     Priority     P      State        Master       VRouter
                                                                  Addr         Addr
---------------         -------  ------------  _      --------     ------------ ------------
vlan2                   1        100          P      Master       local        12.0.0.2
vlan2                   2        255          P      Master       local        12.0.0.1
```

Related Command(s)

- `router vrrp` – Enables VRRP in the router.
- `interface` – Selects an interface to be configured.
- `vrrp - ipv4 address / vrrp – ip address` – Sets the IP address for the virtual router.
- `vrrp group shutdown` – Shuts down all VRRP groups.
- `vrrp – preempt` - Enables the pre-emption of state change from either Backup to Master or vice versa based on the election process.
- `vrrp - text-authentication / vrrp - authentication text` - Sets the authentication type for the virtual router to simple password.
- `vrrp - interval / vrrp - timers advertise` - Sets the advertisement timer for a virtual router.

show vrrp interface

Command Objective This command displays the VRRP status information for all VR-ids created on that interface.

Syntax **show vrrp interface [{ vlan <vlan-id/vfi-id> | <interface- type> <interface-id> | <IP-interface-type> <IP-interface- number>}] [{brief|detail |statistics}]**

Parameter Description

- `vlan <vlan-id/vfi-id>` - Displays the VRRP status information for the specified VLAN/ VFI ID. This value ranges between 1 and 65535.
    - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
    - `<vfi-id>.` - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

      Notes:

      1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.

2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- `<interface-type>` - Displays the VRRP status information for the specified type of interface. The interface can be:
  - `qx-ethernet` **–**A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` **–** A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet`**–** A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Displays the VRRP status information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1.
- `<IP-interface-type>` - Displays VRRP related configuration for the specified L3 Psuedo wire interface in the system.
- `<IP-interface-number>` - Displays VRRP related configuration for the specified interface identifier. This is a unique value that represents the specific interface . This value ranges between 1 and 65535 for Psuedowire interface. This interface type is not supported.

  Note: Maximum number of PseudoWire interfaces supported in the system is 100.

- `brief` - Displays the brief VRRP status information for the specified interface.
- `detail` - Displays the detailed VRRP status information for the specified interface.
- `statistics` - Displays the statistical information for the VRRP for the specified interface.

Mode Privileged EXEC Mode

Example

```
Your Product# show vrrp interface
P indicates configured to preempt
Interface               vrID     Priority      P      State  Master Addr   VRouterAddr
------------------      -------  -----------   -      --------  -----------------  -----------------
Slot0/1                    1     100           P      Master local         21.0.0.1
```

Related Command(s)

- `router vrrp` – Enables VRRP in the router.
- `interface` – Selects an interface to configure.
- `vrrp - ipv4 address / vrrp - ip address` – Sets the IP address for the virtual router
- `vrrp group shutdown` – Shuts down all VRRP groups.
- `vrrp - preempt` - Enables the pre-emption of state change from either Backup to Master or vice versa based on the election process.

auth-deprecate

Command Objective This command enables or disables the Auth Deprecation flag.

Syntax **auth-deprecate { enable | disable }**

Parameter Description

- `enable` - Enables the AuthDeprecation flag.
- `disable` - Disables the AuthDeprecation flag.

Default enable

Mode VRRP Router Configuration Mode

Example

```
Your product(config-vrrp)# auth-deprecate enable
```

debug ip vrrp

Command Objective This command enables the tracing of the VRRP module as per the configured debug levels. The trace statements are generated for the configured trace levels.

This command does not allow combination of debug levels to be configured (that is, more than one level of trace cannot be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

The no form of this command disables the tracing of the VRRP module as per the configured debug levels. The trace statements are not generated for the configured trace levels.

Syntax **debug ip vrrp { all | init | pkt | timers | events | failures }**

no debug ip vrrp { all | init | pkt | timers | events | failures }

Parameter Description

- `all` - Generates debug statements for all kinds of traces.
- `init` - Generates debug statements for init and shutdown traces. This trace is generated

on failed and successful initialization and shutting down of VRRP related module and memory.

- `pkt` - Generates debug statements for packet dump traces. This trace is generated for all events generated during processing of packets.
- `timers` - Generates debug statements for timer traces.
- `events` - Generates debug statements for event traces. This trace is generated when any of packets are sent successfully or when an ACK is received.
- `failures` - Generates debug statements for all kind of failure traces.

Mode User Exec Mode / Privileged EXEC Mode

Example

```
Your product # debug ip vrrp all
```

22 IP

IP (Internet Protocol) is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. example: 10.5.25.180.

Every computer that communicates over the Internet is assigned an IP address that uniquely identifies the device and distinguishes it from other computers on the Internet. Within an isolated network, IP addresses can be assigned at random as long as each one is unique. However, to connect a private network to the Internet, the registered IP addresses must be used (called Internet addresses) to avoid duplicates. The four numbers in an IP address are used in different ways to identify a particular network and a host on that network.

Four regional Internet registries -- ARIN, RIPE NCC, LACNIC and APNIC -- assign Internet addresses from the following three classes.

- Class A - supports 16 million hosts on each of 126 networks
- Class B - supports 65,000 hosts on each of 16,000 networks
- Class C - supports 254 hosts on each of 2 million networks

The number of unassigned Internet addresses is running out, so a new classless scheme called CIDR (Classless Inter-Domain Routing) is gradually replacing the system based on classes A, B, and C and is tied to adoption of IPv6.

ICMP (Internet Control Message Protocol) is an extension to the IP defined by RFC 792. ICMP supports packets containing error, control, and informational messages. For example the ping command uses ICMP to test an Internet connection.
The IP commands under this section are therefore classifiedinto:

- Specific to SMIS IP
- Common to SMIS and Linux IP

22.1 Commands Specific for SMIS IP

This section describes the commands that are specific for SMIS IP alone. These commands are based on the SMIS Proprietary MIB.

The list of CLI commands for the configuration of SMIS IP is as follows:

- ip redirects
- ip unreachables
- ip mask-reply
- ip echo-reply
- maximum-paths
- ip rarp client request
- ip aggregate-route
- traffic-share
- ip path mtu discover
- ip path mtu
- ip rarp client
- ip directed-broadcast
- show ip rarp
- show ip pmtu

ip redirects

Command Objective This command enables sending ICMP Redirect messages. The Redirect Message is an ICMP message which informs a host to update its routing information to send packets on an alternate route when a packet enters an IP interface and exits the same interface. The redirect message is sent to inform the host of the presence of alternative route.

The no form of this command disables sending ICMP Redirect messages.

Syntax **ip redirects [vrf <vrf-name>]**

no ip redirects [vrf <vrf-name>]

Parameter Description `vrf <vrf-name>` - Sends the ICMP redirect messages for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Mode Global Configuration Mode

Default Sending of ICMP Redirect messages is enabled

Note: VRF instance should be created, before executing this command to configure ICMP redirect messages for the context.

Example `Your Product(config)# ip redirects`

Related Command(s)

- `ip vrf` - Creates VRF instance
- `show ip information` -– Displays IP configuration information

ip unreachables

Command Objective This command enables the router to send an ICMP unreachable message to the source if the router receives a packet that has an unrecognized protocol or no route to the destination address. ICMP provides a mechanism that enables a router or destination host to report an error in data traffic processing to the original source of the packet. This informs the source that the packet is dropped.

The no form of this command disables sending ICMP unreachable messages.

Syntax **ip unreachables [vrf <vrf-name>]**

no ip unreachables [vrf <vrf-name>]

Parameter Description `vrf <vrf-name>` - Sends an ICMP unreachable message for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Mode Global Configuration Mode

Package Workgroup, Enterprise, Metro_E and Metro

Note: VRF instance should be created, before executing this command to configure the ICMP unreachable message for the context

Example `Your Product(config)# ip unreachables`

Related Command(s)

- `ip vrf` - Creates VRF instance
- `show ip information` -– Displays IP configuration information

ip mask-reply

Command Objective This command enables sending ICMP Mask Reply messages. The IP mask reply is an ICMP message sent by the router to the host informing the subnet mask of the network. This reply is in correspondence to a request sent by the host seeking the subnet mask of the network.

The no form of this command disables sending ICMP Mask Reply messages.

Syntax **ip mask-reply [vrf <vrf-name>]**

no ip mask-reply [vrf <vrf-name>]

Parameter Description `vrf<vrf-name>`- Sends ICMP mask reply messages for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Mode Global Configuration Mode

Default Sending of ICMP Mask Reply messages is enabled

Note: VRF instance should be created, before executing this command to configure the ICMP mask reply messages for the context.

Example

```
Your Product(config)# ip mask-reply
```

Related Command(s)

- `ip vrf` - Creates VRF instance
- `show ip information` -– Displays IP configuration information

ip echo-reply

Command Objective This command enables sending ICMP Echo Reply messages. The ip echo reply is a message sent by a device, in response to a request sent by another device. This message is used to check if device is able to communicate (send and receive data) with the destination device.

The no form of this command disables sending ICMP Echo Reply messages.

Syntax **ip echo-reply [vrf <vrf-name>]**

no ip echo-reply [vrf <vrf-name>]

Parameter Description `vrf<vrf-name>` - Sends an ICMP Echo reply messages for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Mode Global Configuration Mode

Default Sending of ICMP Echo Reply messages is enabled

Note: VRF instance should be created, before executing this command to configure the ICMP echo reply messages for the context.

Example

```
Your Product(config)# ip echo-reply
```

Related Command(s)

- `ip vrf` - Creates VRF instance
- `show ip information` -– Displays IP configuration information

maximum-paths

Command Objective This command sets the maximum number of paths that can be connected to a host. It provides multiple forwarding paths for data traffic and enables load balancing. It improves the overall network fault tolerance, as failure in one instance does not affect the other instances.

The no form of this command sets the maximum number of paths to its default value.

Note: This command is currently not supported on some models.

Syntax **maximum-paths [vrf <vrf-name>] <value (1-16)>**

no maximum-paths [vrf <vrf-name>]

Parameter Description `vrf<vrf-name>` - Sets the maximum number of paths for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Mode Global Configuration Mode

Default Maximum number of multipaths is set as 2

Note: VRF instance should be created, before executing this command to configure the maximum number of multipaths for the context.

Example

```
Your Product(config)# maximum-paths 15
```

Related Command(s)

- `ip vrf` - Creates VRF instance
- `show ip information` -– Displays IP configuration information

ip rarp client request

Command Objective This command sets the number of RARP client request retries or interval between requests. The ip rarp client request is sent from a newly set up machine in a network. The RARP client program requests the RARP server in the Router to send its IP address. The network administrator creates a table in the lan's gateway router. The router maps the MAC address of the client to an IP address that is sent to the client for future use. If the server didn't respond with an ip address, the client retries the request for configured number of times and the interval between each retry can also be set.

The no form of this command sets the RARP client request retries or interval between retries to the default values.

RARP requests are most commonly sent by diskless clients and JumpStart clients during bootup. The client uses the RARP protocol to broadcast the Ethernet address and asks for the corresponding IP address.

Syntax **ip rarp client request {interval <timeout (30-3000)> | retries <retries (2-10)>}**

no ip rarp client request { interval|retries }

Parameter Description

- `interval <timeout (30-3000)>` - Configures the interval (in seconds) after which an unanswered RARP request is transmitted. The value ranges between 30 and 3000.
- `retries <retries (2-10)>` - Sets the maximum number of retransmissions of RARP request packet after which request must not be sent. The value ranges between 2 and 10.

Mode Global Configuration Mode

Default

- interval 100
- retries 4

Example

```
Your Product(config)# ip rarp client request interval 30
```

Related Command(s) `show ip rarp` - Displays RARP configuration information

ip aggregate-route

Command Objective This command sets the maximum number of aggregate routes. Aggregate Route-based IP switching is achieved by creating a virtual circuit along the network by selecting the forwarding paths used by routers that use OSPF and BGP (Border Gateway Protocol). The data is sent through these virtual circuit to the destination. The routing process is skipped along this circuit. The data is tagged with a label that is read by the switches and forwarded to the destination. This value ranges between 5 and 4095.

The no form of this command sets the maximum number of aggregate routes to its default value.

Syntax **ip aggregate-route <value (5-4095)>**
no ip aggregate-route

Mode Global Configuration Mode

Default 10

Example

```
Your Product(config)# ip aggregate-route 500
```

Related Command(s) `show ip information` -– Displays IP configuration information

traffic-share

Command Objective This command enables traffic sharing (load sharing of IP packets). Traffic sharing is the process by which the protocols select the route for traffic flow with regard to path cost calculation and load distribution. EIGRP (Enhanced Interior Gateway Routing Protocol) provides intelligent traffic sharing.

Traffic sharing is controlled by selecting the Mode of distribution. Traffic-share balanced distributes the traffic proportionately to the ratio of the metrics of different routes. The Traffic-share min distributes the traffic in the route which has minimal cost path even if different paths are available.

The no form of this command disables traffic sharing.

Note: This command is currently not supported on some models.

Syntax **traffic-share [vrf <vrf-name>]**

no traffic-share [vrf <vrf-name>]

Parameter Description `vrf<vrf-name>`- Enables traffic sharing for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Mode Global Configuration Mode

Default Load Sharing is disabled

Note: VRF instance should be created, before executing this command to configure the traffic sharing for the context.

Example

```
Your Product(config)# traffic-share
```

Related Command(s)

- `ip vrf` - Creates VRF instance
- `show ip information` -– Displays IP configuration information

ip path mtu discover

Command Objective This command initiates path MTU (Maximum Transmission Unit) discovery.

The no form of this command sets path MTU discovery to its default value. When IP path MTU discover is set to be disabled, PMTU-D is not done even if the application requests to do so.

Syntax **ip [vrf <vrf-name>] path mtu discover**
no ip [vrf <vrf-name>] path mtu discover

Parameter Description `vrf<vrf-name>` - Initiates path MTU for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Mode Global Configuration Mode

Default Path MTU discovery is disabled

Note: VRF instance should be created, before executing this command to configure the path MTU discovery for the context.

Example Your Product(config)# ip path mtu discover

Related Command(s)

- `ip path mtu` - Sets the MTU for usage in PMTU Discovery
- `ip vrf` - Creates VRF instance
- `show ip information` -– Displays IP configuration information

ip path mtu

Command Objective This command sets the MTU for usage in PMTU discovery. The transmission of packets from source to destination has many networks to pass through. Each network has its own Maximum transmission unit. The smallest MTU of all the links is the path MTU. This PMTU can be manually configured by the administrator.

The no form of this command removes MTU for usage in PMTU Discovery.

Syntax **ip path mtu [vrf <vrf-name>] <dest ip> <tos> <mtu(68-65535)>**

no ip path mtu [vrf <vrf-name>] <dest ip> <tos>

Parameter Description

- `vrf<vrf-name>` - Sets the MTU for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
- `dest ip` - Sets the Destination IP Address. This is done to define the path between source and destination.
- `tos` - Sets the Type of Service of the configured route
- `mtu` - Sets the Maximum Transmission Unit for the path from source to the destination. This value ranges between 68 and 65535.

Mode Global Configuration Mode

Notes:

- Path MTU discovery needs to be enabled to execute this command.
- VRF instance should be created, before executing this command to configure the MTU for the context

Example

```
Your Product(config)# ip path mtu 10.0.0.1 0 1800
```

Related Command(s)

- `ip vrf` - Creates VRF instance
- `ip path mtu discovery` - Enables path mtu (Maximum Transmission Unit) discovery
- `show ip pmtu` - Displays the configured PMTU Entries

ip rarp client

Command Objective This command enables RARP (Reverse Address Resolution Protocol) client. The RARP resolves an IP address from a given hardware address. The client that requests for the IP is the RARP client. The IP address of the default interface is obtained through RARP, when the IP address configuration Mode is dynamic. After RARP Max retries, IP is obtained through DHCP.

The no form of this command disables RARP client.

Note: This command is currently not supported in the code.

Syntax **ip rarp client**

no ip rarp client

Mode Interface Configuration Mode

Default Enabled

Note: The RARP server must be disabled when the RARP client is enabled.

Example

```
Your Product(config-if)# ip rarp client
```

Related Command(s)

- `show interfaces` - Displays the interface status and configuration for all interfaces available in the switch.
- `show ip rarp` - Displays RARP configuration information.

ip directed-broadcast

Command Objective This command enables forwarding of directed broadcasts. The IP directed broadcast is an IP packet whose destination is a valid IP subnet address, but the source is from a node outside the destination subnet. The routers from outside the subnet forwards the IP directed broadcast, like any other IP packet. When the directed packets reach a router in the destination subnet, the packet is exploded as a broadcast in the subnet. The header information on the broadcast packet is rewritten for the broadcast address in the subnet. The packet is sent as link-layer broadcast.

The no form of this command disables forwarding of directed broadcasts.

Syntax **ip directed-broadcast**

no ip directed-broadcast

Mode Vlan Interface Configuration Mode

Default Disabled

Example

```
Your Product(config-if)# ip directed-broadcast
```

Related Command(s) `show interfaces` - Displays the interface status and configuration for all interfaces available in the switch.

show ip rarp

Command Objective This command displays RARP configuration information. RARP Configurations such as Maximum number of RARP request retransmission retries and RARP request retransmission timeout. It also displays the number of responses discarded.

Syntax **show ip rarp**

Mode Privileged EXEC Mode

Example

```
Your Product# show ip rarp
RARP Configurations:
--------------------------------
Maximum number of RARP request retransmission retries is
4
RARP request retransmission timeout is 100 seconds
RARP Statistics:
-------------------------
0 responses discarded
```

Related Command(s)

- `ip rarp client request` - Sets the number of RARP client request retries
- `ip rarp client` - Enables RARP client

show ip pmtu

Command Objective This command displays the configured PMTU entries. The details include Destination IP address, Type of Service and Path MTU.

Syntax **show ip pmtu [vrf <vrf-name>]**

Parameter Description `vrf <vrf-name>` - Sends an ICMP unreachable message for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Mode Privileged EXEC Mode

Package Workgroup, Enterprise, Metro_E and Metro

Default vrf - default

Example

```
Your Product# show ip pmtu
Ip Path MTU Table
---------------------------
Vrf Name                    Destination      TOS     PMTU
---------------------   ---------------      ---     ----

Default                     15.0.0.20        0       1500
vr1                         14.0.0.25        0       900
Your Product# show ip pmtu vrf vr1
Ip Path MTU Table
---------------------
Vrf Name                    Destination      TOS     PMTU
--------                    -----------      ---     ----
vr1                         14.0.0.25        0       900
```

Related Command(s) `ip path mtu` - Sets the MTU for usage in PMTU Discovery

22.2 Commands Common for Aricent and Linux IP

This section describes the commands that are common for SMIS IP and Linux IP. These commands are based on the standard MIB.

The list of CLI commands for the configuration of SMIS and Linux IP is as follows:

- ping
- ip route
- ip routing
- ip default-ttl
- arp timeout
- arp – ip address
- ip arp max-retries
- ip proxyarp-subnetoption
- ipv4 enable
- ip proxy-arp
- show ip traffic
- show ip information
- show ip route
- show ip arp
- show ip proxy-arp

ping

Command Objective This command sends echo messages. The Packet Internet Groper (Ping) module is built based on the ICMP echo request and ICMP echo response messages. The network administrator uses this ping on a remote device to verify its presence. Ping involves sending ICMP echo messages repeated and measuring the time between transmission and reception of message. The output displays the time taken for each packet to be transmitted, number of packets transmitted, number of packets received and packet loss percentage.

Syntax **ping [vrf <vrf-name>] [ip] {IpAddress | hostname } [data (0-65535)] [df-bit] [{repeat|count} packet_count (1-10)] [size packet_size (36-2080)][source <ip-address>] [timeout time_out (1-100)] [validate]**

Parameter Description

- `vrf<vrf-name>` - Configures IP for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
- `ip` - Configures the IP address of the node to be pinged.
- `IpAddress` - Configures the source IP address of the node to be pinged.
- `hostname` - Configures the name of the host.
- `data (0-65535)` - Configures the size of the data. The value ranges between 0 and 65535.
- `df-bit` - Configures Dont Fragment (DF) bit on the ping packet.
- `repeat` - Configures number of ping messages.
- `count` - Configures the number of times the given node address is to be pinged.
- `packet_count (1-10)` - Configures the packet count. The value ranges between 1 and 10
- `size packet_size (36-2080)` - Configures the size of the data portion of the PING PDU. This value ranges between 0 and 2080.
- `source <ip-address>` - Configures the source IP address of the router for the probes.
- `timeout time_out (1-100)` - Configures the time in seconds after which the entity waiting for the ping response times out. The value ranges between 1 and 100.
- `validate` - Validates the reply data.
- `destination-address` - Configures the destination IP address of the router for the probes.

Mode Privileged EXEC Mode

Default

- size packet_size 500
- count packet_count 3
- timeout time_out 5

Note: VRF instance should be created, before executing this command to send echo message for the context

Example

```
Your Product# ping 10.0.0.2
Reply Received From :10.0.0.2, TimeTaken : 20 msecs
Reply Received From :10.0.0.2, TimeTaken : 10 msecs
Reply Received From :10.0.0.2, TimeTaken : 10 msecs
--- 10.0.0.2 Ping Statistics ---
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
```

Related Command(s) `ip vrf - Creates VRF instance.`

ip route

Command Objective This command adds a static route. The Route defines the IP address or interface through which the destination can be reached.

The no form of this command deletes a static route.

Note: If the static route is configured without any metric value, then the route will be configured with metric value 1.

Syntax **ip route [vrf <vrf-name>] <prefix> <mask> {<next-hop> | Vlan <vlan-id/vfi-id> [switch <switch-name>] | <interface- type> <interface-id> | Linuxvlan <interface-name> | Cpu0 | tunnel <tunnel-id (0-128)> | <IP-interface-type> <IP- interface-number>} [<distance (1-254)>] [private] [permanent] [name <nexthop-name>]**

no ip route [vrf <vrf-name>] <prefix> <mask> [{ <next-hop> | Vlan <vlan-id/vfi-id> [switch <switch-name>] | <interface-type> <interface-id> | Linuxvlan <interface-name> | Cpu0 | tunnel <tunnel-id (0-128)>} | <IP- interface-type> <IP-interface-number>] [private] [permanent] [name <nexthop-name>]

Parameter Description

- vrf<vrf-name> - Adds a static route for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
- <prefix> - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network.
- <mask> - Configures the subnet mask for the IP address. This is a 32-bit number which is used to divide the IP address into network address and host address.
- <next-hop> - Defines the IP address or IP alias of the next hop that can be used to reach that network.
- Vlan <vlan-id/vfi-id> - Adds a static route for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
    - vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
    - <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

    Notes:

    1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
    2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
    3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of

VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- `switch<switch-name>` - Adds a static route for the specified context. This value represents unique name of the switch context. feature. This value is a string whose maximum size is 32.
- `<interface-type>` - Adds a static route for the specified type of interface. The interface can be:
    - `fastethernet` – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer upto 100 Megabits per second.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `i-lan`– Internal LAN created on a bridge per IEEE 802.1ap.
- `<interface-id>` - Adds a static route for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For example: 0/1 represents that the slot number is 0 and port number is 1.
- `Linuxvlan<interface-name>` - Defines the Interface Name of the Linux VLAN Interface
- `Cpu0` - Sets the Out of Band Management Interface for the route
- `tunnel<id>` - Adds a static route for the specified Tunnel Identifier. This value ranges between 0 and 128.
- `<IP-interface-type>` - Adds a static route for the specified L3 Psuedo wire interface in the system.
- `<IP-interface-number>` - Adds a static route for the specified L3 Psuedo wire interface identifier. This is a unique value that represents the specific interface. This value ranges between 1 and 65535 for Psuedowire interface.

  Note: Maximum number of PseudoWire interfaces supported in the system is 100.

- `<distance (1-254)>` - Defines the Administrative distance as per the metrics. This value ranges between 1 and 254.
- `private` - Sets the Private route
- `permanent` - Sets the permenant route.
- `name <nexthop-name>` - Configures next hop name fpr the newly added static route.

Mode Global Configuration Mode

Default distance - -1

Notes:

- When the next-hop object is unknown or not relevant its value must be set to zero.
- Interface must be a router port.
- VRF instance should be created, before executing this command to add static route for the context.

- VRF instance should be mapped to the IPV4 / IPV6 interface, before executing this command to add the static routes for the context in the interface.

Example `Your Product(config)# ip route 30.0.0.2 255.255.255.255 Vlan 1`

Related Command(s)

- `ip vrf` - Creates VRF instance.
- `ip vrf forwarding` - Maps the IPV4 / IPV6 interface to the context.
- `show ip route` - Displays the IP routing table.
- `no switchport` – Configures the port as a router port.

ip routing

Command Objective This command enables IP routing. IP routing is the path defined by set of protocols for the data to follow across multiple networks from source to its destination. When an IP packet is to be forwarded, the router uses its forwarding table to determine the next hop address for the packet to reach its destination. The header in the IP packet consists of the next hop information.

The no form of this command disables IP routing.

Syntax **ip routing [vrf <vrf-name>]**

no ip routing [vrf <vrf-name>]

Parameter Description `vrf<vrf-name>`- Enables IP routing for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Mode Global Configuration Mode

Default IP routing is enabled

Note: VRF instance should be created, before executing this command to configure IP routing for the context.

Example `Your Product(config)# ip routing`

Related Command(s)

- `ip vrf` -Creates VRF instance
- `show ip information` - Displays IP configuration information
- `show ip route` - Displays the IP routing table

ip default-ttl

Command Objective This command sets the Time-To-Live (TTL) value. TTL is the time set for a unit of data (a packet) to remain in the network or computer before it could be discarded. This value ranges between 1 and 255 seconds.

The no form of this command sets the TTL to the default value.

Syntax **ip default-ttl [vrf <vrf-name>] <value (1-255)>**

no ip default-ttl [vrf <vrf-name>]

Parameter Description `vrf<vrf-name>`- Sets the Time-To-Live (TTL) value for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Mode Global Configuration Mode

Default 64 seconds

Note: VRF instance should be created, before executing this command to configure TTL value for the context.

Example

```
Your Product(config)# ip default-ttl 1
```

Related Command(s)

- `ip vrf` -Creates VRF instance
- `show ip information` - Displays IP configuration information

arp timeout

Command Objective This command sets the ARP (Address Resolution Protocol) cache timeout.

The arp timeout defines the time period an arp entry remains in the cache. When a new timeout value is assigned, it only affects the new arp entries. All the older entries retain their old timeout values. The timeout values can be assigned to dynamic arp entries only. All static arp entries remain unaltered by the timeout value. This value ranges between 30 and 86400 seconds.

The no form of this command sets the ARP cache timeout to its default value.

Syntax **arp [vrf <vrf-name>] timeout <seconds (30-86400)>**

no arp [vrf <vrf-name>] timeout

Parameter Description `vrf <vrf-name>` - Sets the ARP cache timeout for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Mode Global Configuration Mode

Default 7200

Note: VRF instance should be created, before executing this command to configure ARP cache timeout for the context.

Example

```
Your Product(config)# arp timeout 35
```

Related Command(s)

- `ip vrf` - Creates VRF instance
- `show ip arp` - Displays IP ARP table for the given VLAN ID/IP Address of ARP entry/MAC Address of ARP entry/IP ARP summary table/ARP configuration information

arp – ip address

Command Objective This command adds a static entry in the ARP cache. The ARP finds the hardware address of the client and stores them in arp cache. The arp entry can be configured manually by using this command. The entry is stored permanently in the arp cache as a static entry.

The no form of this command deletes a static entry from the ARP cache.

Syntax **arp [vrf <vrf-name>] <ip address> <hardware address> {Vlan <vlan-id/vfi-id> [switch switch-name] | <interface-type> <interface-id> | Linuxvlan <interface-name>| Cpu0 | <IP- interface-type> <IP-interface-number>}**

no arp [vrf <vrf-name>] <ip address>

Parameter Description

- `vrf<vrf-name>` - Adds a static entry in the ARP cache for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
- `<ip address>` - Defines the IP address or IP alias to map to the specified MAC address.
- `<hardware address>` - Defines the MAC address to map to the specified IP address or IP alias.
- `Vlan <vlan-id/vfi-id>` - Adds a static entry in the ARP cache for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535.

  Notes:

  1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries. This interface type is not supported.
  2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
  3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- `switch <switch-name >` - Adds a static entry in the ARP cache for the specified context. This value

represents unique name of the switch context. feature. This value is a string whose maximum size is 32. It is specific to multiple instance feature.

- `<interface-type>` - Adds a static static entry in the ARP cache for the specified interface.
  - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Adds a static static entry in the ARP cache for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that the slot number is 0 and portnumber is 1. Only port-channel ID is provided, for interface type port-channel. For example:1 represents port-channel ID.
- `Linuxvlan<interface-name>` - Sets the Linux VLAN Interface
- `Cpu0` - Sets the Out of Band Management Interface for the route.
- `<IP-interface-type>` - Adds a static static entry in the ARP cache for the specified L3 Psuedo wire interface in the system.
- `<IP-interface-number>` - Adds a static static entry in the ARP cache for the specified L3 Psuedo wire interface identifier. This is a unique value that represents the specific interface . This value ranges between 1 and 65535 for Psuedowire interface.

Note: Maximum number of PseudoWire interfaces supported in the system is 100.

Mode Global Configuration Mode

Notes:

- Interface must be a router port.
- VRF instance should be created, before executing this command to add static entry for the context.
- VRF instance should be mapped to the IPV4 / IPV6 interface, before executing this command to add static entry for the context in the interface.

Example

```
Your Product(config)# arp 10.203.120.21
00:11:22:33:44:55 Vlan 1
```

Related Command(s)

- `ip vrf` - Creates VRF instance
- `ip vrf information` - Maps the IPV4 / IPV6 interface to the context
- `show ip arp` - Displays IP ARP table for the given VLAN ID/IP Address of ARP entry/MAC Address of ARP entry/IP ARP summary table/ARP configuration information

- `no switchport` - Configures the port as a router port

ip arp max-retries

Command Objective This command sets the maximum number of ARP request retries. The maximum number of ARP requests that the switch generates before deleting an un-resolved ARP entry isdefined.

The no form of this command sets the maximum number of ARP request retries to its default value.

Syntax **ip arp [vrf <vrf-name>] max-retries <value (2-10)>**

no ip arp [vrf <vrf-name>] max-retries

Parameter Description

- `vrf<vrf-name>` - Sets maximum number of ARP request retries for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is32.
- `<value (2-10)>` - Configures the maximum number of ARP request entries.The value ranges between 2 and 10.

Mode Global Configuration Mode

Default 3

Note: VRF instance should be created, before executing this command to configure the maximum number of ARP request retries for the context.

Example

```
Your Product(config)# ip arp max-retries 2
```

Related Command(s)

- `ip vrf` - Creates VRF instance
- `show ip arp` - Displays IP ARP table for the given VLAN ID/IP Address of ARP entry/MAC Address of ARP entry/IP ARP summary table/ARP configuration information

ip proxyarp-subnetoption

Command Objective This command enables proxy ARP subnet check. ISS acts as ARP proxy for target address in different subnet, when subnet check is enabled.

The no form of the command disables proxy ARP subnet check,. ISS acts as ARP proxy for target address in same or different subnet that is used in IP- DSLAM (Digital Subscriber Line Access Multiplexer) case, when subnet check is disabled.

Syntax **ip proxy-arp-subnetoption**

no ip proxy-arp-subnetoption

Mode Global Configuration Mode

Default Proxy ARP subnet check is enabled.

Example `Your Product(config)# ip proxy-arp-subnetoption`

ipv4 enable

Command Objective This command enables IPv4 processing on the interface that has not been configured with an explicit IPv4 address.

The no form of this command disables IPv4 processing on the interface.

Syntax **ipv4 enable**

no ipv4 enable

Mode Interface Configuration Mode (Vlan)

Default enable

Example Your Product(config-if)# ipv4 enable

Related Command(s) `show ip information` - Displays IP configuration information

ip proxy-arp

Command Objective This command enables proxy ARP for the interface.

The no form of the command disables proxy ARP for the interface.

Syntax **ip proxy-arp**

no ip proxy-arp

Mode Interface Configuration Mode (Vlan)

Default Proxy ARP is disabled.

Example `Your Product(config-if)# ip proxy-arp`

Related Command(s) `show ip proxy-arp` - Displays the status of the proxy ARP for all the created interfaces.

show ip traffic

Command Objective This command displays the IP protocol statistics.

Syntax **show ip traffic [vrf <vrf-name>] [interface { Vlan<vlan- id/vfi-id> [switch <switch-name>]**

| tunnel <tunnel-id (1-128)> | <interface-type> <interface-id> | Linuxvlan <interface-name> | <IP-interface-type> <IP-interface-number> }] [hc]

Parameter Description

- `vrf<vrf-name>` - Displays the IP protocol statistics information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is32.
- `Vlan <vlan-id/vfi-id>` - Displays the ip protocol statistics for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
    - <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
    - <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

    Notes:

    1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
    2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
    3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- `switch<switch-name>` - Displays the IP protocol statistics information for the specified context. This value represents unique name of the switch context. feature. It is specific for multiple instance feature.
- `tunnel<tunnel-id (1-128)>` - Displays the Tunnel identifier. The value ranges between 1 and 128.
- `<interface-type>` - Displays the IP protocol statistics information for the specified interface type. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Displays the interface id. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided for interface type port-channel. Forexample: 1 represents port-channel ID.

- `Linuxvlan <interface-name>` - Displays the Linux IP Vlan identifier
- `<IP-interface-type>` - Displays the IP statistics for the specified L3 Psuedo wire interface in the system.
- `<IP-interface-number>` - Displays the IP statistics for the specified L3 Psuedo wire interface identifier. This is a unique value that represents the specific interface. This value ranges between 1 and 65535 for Psuedowire interface.

  Note: Maximum number of PseudoWire interfaces supported in the system is 100.

- `hc` - Displays the High counters statistics information.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip traffic
VRF Name:         default
---------------- IP Statistics
--------------------
Rcvd: 0 total, 0 header error discards
0 bad ip address discards, 0 unsupported protocol discards
Frags:                  0 reassembled, 30 timeouts, 0 needs reassembly
0 fragmented, 0 couldn't fragment
Bcast: Sent: 0 forwarded, 0 generated requests
Drop:
0                       InDiscards      0      InDelivers          0     InMcastPkts
0                       InTruncated     0      InOctets            0     InNoRoutes
0                       ReasmFails      0      InMcast Octets            0
                        InBcastPkts
0                       OutDiscards     0      OutMcastPkts        0     OutFrgCreates
0                       OutForwDgrms    0      OutTrnsmits         0     OutFrgRqds
0                       OutOctets 0            OutMcstOctets       0     OutBcstPkts
0                       DiscntTime             1000 RefrshRate
ICMP Statistics:
----------------
Rcvd:                   0 total, 0 checksum errors, 0 unreachable, 0 redirects
                        0 time exceeded, 0 param problems, 0 quench
                        0 echo, 0 echo reply, 0 mask requests, 0 mask replies,
                        0 timestamp , 0 time stamp reply,
Sent:                   0 total, 0 checksum errors, 0 unreachable, 0 redirects
                        0 time exceeded, 0 param problems, 0 quench
                        0 echo, 0 echo reply, 0 mask requests, 0 mask replies,
                        0 timestamp , 0 time stamp reply, VRF Name:         vr1
----------------
IP Statistics
--------------------
Rcvd:                   0 total, 0 header error discards
                        0 bad ip address discards, 0 unsupported protocol discards
Frags:                  0 reassembled, 30 timeouts, 0 needs reassembly
                        0 fragmented, 0 couldn't fragment
Bcast: Sent:            0 forwarded, 0 generated requests
Drop:
                        0  InDiscards   0  InDelivers      0  InMcastPkts
                        0  InTruncated  0  InOctets        0  InNoRoutes
                        0  ReasmFails   0  InMcast Octets  0  InBcastPkts
                        0  OutDiscards  0  OutMcastPkts    0  OutFrgCreates
                        0  OutForwDgrms 0  OutTrnsmits     0  OutFrgRqds
                        0  OutOctets    0  OutMcstOctets   0  OutBcstPkts
                        0  DiscntTime   1000 RefrshRate
                        ICMP Statistics:
-------------------------
Rcvd:                   0 total, 0 checksum errors, 0 unreachable, 0 redirects
                        0 time exceeded, 0 param problems, 0 quench
                        0 echo, 0 echo reply, 0 mask requests, 0 mask replies,
                        0 timestamp , 0 time stamp reply,
Sent:                   0 total, 0 checksum errors, 0 unreachable, 0 redirects
                        0 time exceeded, 0 param problems, 0 quench
                        0 echo, 0 echo reply, 0 mask requests, 0 mask replies,
                        0 timestamp , 0 time stamp reply,
Your Product# show ip traffic vrf vr1
VRF Name:         vr1
-------------------------
IP Statistics
--------------------------------
Rcvd:                   0 total, 0 header error discards
                        0 bad ip address discards, 0 unsupported protocol discards
Frags:                  0 reassembled, 30 timeouts, 0 needs reassembly
                        0 fragmented, 0 couldn't fragment
Bcast: Sent:            0 forwarded, 0 generated requests
Drop:
                        0  InDiscards   0  InDelivers      0  InMcastPkts
                        0  InTruncated  0  InOctets        0  InNoRoutes
                        0  ReasmFails   0  InMcast Octets  0  InBcastPkts
                        0  OutDiscards  0  OutMcastPkts    0  OutFrgCreates
                        0  OutForwDgrms 0  OutTrnsmits     0  OutFrgRqds
                        0  OutOctets    0  OutMcstOctets   0  OutBcstPkts
                        0  DiscntTime      1000 RefrshRate
ICMP Statistics:
-------------------------
Rcvd:                   0 total, 0 checksum errors, 0 unreachable, 0 redirects
                        0 time exceeded, 0 param problems, 0 quench
                        0 echo, 0 echo reply, 0 mask requests, 0 mask replies,
                        0 timestamp , 0 time stamp reply,
Sent:                   0 total, 0 checksum errors, 0 unreachable, 0 redirects
                        0 time exceeded, 0 param problems, 0 quench
                        0 echo, 0 echo reply, 0 mask requests, 0 mask replies,
                        0 timestamp , 0 time stamp reply,
```

show ip information

Command Objective This command displays IP configuration information.

Syntax **show ip information [vrf <vrf-name>]**

Parameter Description `vrf <vrf-name>` - Displays the configured IP information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Mode Privileged EXEC Mode

Default vrf - default

Note: For Linux IP, this command displays only the IP Routing status and the default TTL value.

Example

```
Your Product# show ip information
VRF Name:    default
Global IP Configuration:
 IP routing is enabled default TTL is 64
ICMP redirects are always sent
ICMP unreachables are always sent ICMP echo replies are always sent ICMP mask replies
are always sent Number of aggregate routes is 50
Number of multi-paths is 2
Load sharing is disabled
Path MTU discovery is disabled
VRF Name:    vr1
Global IP Configuration:
--------------------------------------
IP routing is enabled default TTL is 64
ICMP redirects are always sent
ICMP unreachables are always sent ICMP echo replies are always sent ICMP mask replies
are always sent Number of aggregate routes is 50
Number of multi-paths is 2
Load sharing is disabled
Path MTU discovery is disabled
Your Product# show ip information vrf vr1
VRF Name:    vr1
Global IP Configuration:
--------------------------------------
IP routing is enabled default TTL is 64
ICMP redirects are always sent ICMP unreachables are always sent ICMP echo replies are
always sent ICMP mask replies are always sent Number of aggregate routes is 50
Number of multi-paths is 2
Load sharing is disabled
Path MTU discovery is disabled
```

Related Command(s)

- `ip redirects` - Enables sending ICMP
- `ip unreachable` - Enables sending ICMP unreachable message
- `ip mask-reply` - Enables sending ICMP Mask Reply messages
- `ip echo-reply` - Enables sending ICMP Echo Reply messages
- `maximum-paths` - Sets the maximum number of multipaths
- `ip aggregate-route` - Sets the maximum number of aggregate routes
- `ip path mtu discover` - Enables path mtu discovery
- `traffic-share` - Enables traffic sharing

- `ip routing` – Enables IP routing
- `ip default-ttl` - Sets the Time-To-Live (TTL) value.
- `ipv4 enable` - Enables IPv4 processing on the interface

show ip route

Command Objective This command displays the IP routing table.

Syntax **show ip route [vrf <vrf-name>] [{ <ip-address> [<mask>] | bgp | connected | ospf | rip | static | summary }]**

Parameter Description

- `vrf<vrf-name>` - Displays the IP routing table for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
- `<ip-address>` - Displays the IP routing table for the specified destination IP Address.
- `<mask>` - Displays the IP routing table for the specified prefix mask address.
- `bgp` - Displays the Border Gateway Protocol if it is used by the table to get route information.
- `connected` - Displays the Directly Connected Network Routes.
- `ospf` - Displays the OSPF (Open Shortest Path First) protocol if it is used for getting route information.
- `rip` - Displays the RIP (Routing Information Protocol) if it is used for getting route information.
- `static` - Displays the Static Routes in the table.
- `summary` - Displays the Summary of all routes.

Mode Privileged EXEC Mode

Default vrf - default

Example

```
Your Product# show ip route
Codes: 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
Vrf Name:          default
---------------
C 12.0.0.0/8 is directly connected, vlan1
O IA 15.0.0.0/8 [2] via 12.0.0.7
O E2 20.0.0.0/8 [10] via 12.0.0.7
Your Product# show ip route vrf vr1
Vrf Name:          vr1
---------------
C 14.0.0.0/8 is directly connected, vlan3
Your Product# show ip route summary
VRF Name:          default
--------------------------
Route SourceRoutes
connected         2
static            0
```

```
rip               0
bgp               0
ospf              2
Total             4
Total ECMP routes 2
```

Related Command(s)

- `ip route` - Adds a static route.
- `ip routing` - Enables IP routing.

show ip arp

Command Objective This command displays IP ARP table.

Syntax **show ip arp [vrf <vrf-name>][{ Vlan <vlan-id/vfi-id> [switch <switch-name>] | <interface-type> <interface-id> | <ipiftype> <ifnum> | <ip-address> | <mac-address> | summary | information | statistics }]**

Parameter Description

- `vrf<vrf-name>` - Displays the IP ARP information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
- `Vlan <vlan-id/vfi-id>` - Displays the IP ARP information for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - `<vfi-id>.` - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

    Notes:

    1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
    2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
    3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- `switch<switch-name>` - Displays the IP ARP information for the specified context. This value represents unique name of the switch context.
- `<interface-type>` - Displays specified type of interface. The interface can be:
  - `qx-ethernet` –A version of Ethernet that supports data transfer upto 40 Gigabits per

second. This Ethernet supports only full duplex links.

  - gigabitethernet **–** A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet **–** A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Displays the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, For example: 0/1 represents that the slot number is 0 and port number is 1.
- `<ipiftype>` - Displays the IP ARP information for the specified L3 Psuedo wire interface in the system.
- `<ifnum>` - Displays the IP ARP information for the specified L3 Psuedo wire interface identifier. This is a unique value that represents the specific interface . This value ranges between 1 and 65535 for Psuedowire interface.

  Note: Maximum number of PseudoWire interfaces supported in the system is 100.

- `<ip-address>` - Displays the IP Address of ARP Entry
- `<mac-address>` - Displays the MAC Address of ARP Entry
- `summary` - Displays IP ARP Table summary
- `information` - Displays the ARP Configuration information regarding maximum retries and ARP cache timeout.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip arp
VRF Id : 0
VRF Name: default
Address        Hardware Address   Type Interface Mapping
-----------    -----------------  ------- ---------- ----------
12.0.0.100       00:1b:11:c2:94:f6 ARPA vlan1    Dynamic
15.0.0.10        00:03:02:03:01:04 ARPA vlan2    Static
VRF Id : 1
VRF Name: vr1
Address       Hardware Address   Type Interface Mapping
-----------   -----------------  ------- ---------- ----------
14.0.0.10     00:04:02:03:01:04 ARPA vlan3      Static
Your Product# show ip arp vrf vr
VRF Id : 1
VRF Name: vr1
Address        Hardware Address   Type Interface Mapping
-----------    -----------------  ------- ---------- ----------
14.0.0.10        00:04:02:03:01:04 ARPA vlan3      Static
Your Product# show ip arp 12.100
Address Hardware Address Type Interface Mapping VRF Name
----------- ----------------- ------- ---------- ---------- -----------
12.0.0.100 00:1b:11:c2:94:f6 ARPA vlan1 Dynamic default
Your Product# show ip arp 00:04:02:03:01:04
```

```
Address Hardware Address Type Interface Mapping VRF Name
14.0.0.10 00:04:02:03:01:04 ARPA vlan1 Static  default
14.0.0.10 00:04:02:03:01:04 ARPA vlan3 Static  vr1
Your Product# show ip arp summar
VRF Name:    default
3 IP ARP entries, with 0 of them incomplete
VRF Name:    vr1
1 IP ARP entries, with 0 of them incomplete
Your Product# show ip arp vrf vr1 summary
VRF Name:    vr1
1 IP ARP entries, with 0 of them incomplete
Your Product# show ip arp information
ARP Configurations:
------------------- VRF Name: default
Maximum number of ARP request retries is 3
ARP cache timeout is 300 seconds
VRF Name: vr1
Maximum number of ARP request retries is 3
ARP cache timeout is 300 seconds
Your Product# show ip arp vrf vr1 information
ARP Configurations:
------------------- VRF Name: vr1
Maximum number of ARP request retries is 3
ARP cache timeout is 300 seconds
```

Related Command(s)

- `arp timeout` - Sets the ARP (Address Resolution Protocol) cache timeout
- `arp – ip address` - Adds a static entry in the ARP cache
- `ip arp max-retries` - Sets the maximum number of ARP request retries

show ip proxy-arp

Command Objective This command displays the status of the proxy ARP for all the created interfaces.

Syntax **show ip proxy-arp [vrf <vrf-name>]**

Parameter Description vrf<vrf-name> - Displays the status of the proxy ARP for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip proxy-arp
PROXY ARP Status
-------------------------
vlan1     : Disabled vlan2     : Disabled vlan3     : Disabled
---------------------------------
Your Product# show ip proxy-arp vrf default
PROXY ARP Status
-------------------------
```

```
vlan1      : Disabled vlan2      : Disabled
---------------------------------
```

Related Command(s) `ip proxy-arp` - Enables proxy ARP for the interface

23 DHCP

DHCP (Dynamic Host Configuration Protocol) is used in a wide variety of devices like ISDN routers, firewalls, etc., for assigning IP addresses to workstations. Besides obtaining IP address, other configuration parameters for a workstation can also be configured in a DHCP server. DHCP clients can retrieve these parameters along with the IP address.

DHCP is based on the client-server architecture. DHCP servers are configured with an IP address and several other configuration parameters. DHCP clients, typically workstations obtain this IP address at start- up. The client obtains the address for a time period termed as the “lease” period. DHCP clients renew the address by sending a request for the IP address before the lease expires.

DHCP uses UDP as its transport protocol and a UDP port for communication. DHCP relay agents connect servers present on one LAN with the client present on another.

23.1 DHCP Client

DHCP client uses DHCP to temporarily receive a unique IP address for it from the DHCP server. It also receives other network configuration information such as default gateway, from the DHCP server.
The list of CLI commands for the configuration of DHCP Client is as follows:

- debug ip dhcp client
- release dhcp
- renew dhcp
- show ip dhcp client stats
- ip dhcp client discovery timer
- ip dhcp client idle timer
- ip dhcp client arp-check timer
- ip dhcp client fast-access
- ip dhcp client client-id
- ip dhcp client request
- show ip dhcp client fast-access
- show ip dhcp client option

debug ip dhcp client

Command Objective This command enables the tracking of the DHCP client operations as per the configured debug levels. The debug statements are generated for the specified trace levels.

The no form of the command disables the tracking of the DHCP client operations. The debug statements are not generated for the specified trace levels.

This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

Syntax **debug ip dhcp client { all | event | packets | errors | bind }**
no debug ip dhcp client { all | event | packets | errors | bind }

Parameter Description

- `all` - Generates debug statements for all kind of failure traces.
- `event` - Generates debug statements for DHCP client events that provide DHCP client service status. The DHCP client events are generated when any of packets are sent successfully or when an ACK is received.
- `packets` - Generates debug statements for packets related messages. These messages are generated for all events generated during processing of packets.
- `errors` - Generates debug statements for trace error code debug messages. These messages are generated for all error events generated.
- `bind` - Generated debug statements for trace bind messages. These messages are generated when a DHCP ACK is received.

Mode Privileged EXEC Mode

Default Tracking of the DHCP client operations is disabled.

Example Your Product# debug ip dhcp client all

Related Command(s) `show debugging` - Displays state of each debugging option

release dhcp

Command Objective This command immediately releases the DHCP lease obtained for an IP address from a DHCP server and assigned to the specified interface. The current lease assigned to that interface is terminated manually.

The lease is terminated to reset the DHCP client which faces connectivity problem. The DHCP lease provided by the DHCP server represents the time interval till which the DHCP client can use the assigned IP address.

Syntax **release dhcp { vlan <vlan-id (1-4094)> | <interface-type> <interface-id> }**

Parameter Description

- `<vlan-id (1-4094)>` - Releases the DHCP lease for the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.

- `vlanMgmt` - Releases the DHCP lease for the management vlan interface.
- `<interface-type>` - Releases the DHCP lease for the specified type of interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Releases the DHCP lease for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents thatthe slot number is 0 and port number is 1. Only port-channel ID is provided for interface type port-channel. For example: 1 represents port-channel ID.

Mode Privileged EXEC Mode

Note: This command executes successfully only if the VLAN interfaces and router ports are in BOUND state (that is, IP address is dynamically acquired from DHCP server and an active lease is bound to the interface). The port should have been configured as router port for dynamically acquiring an IP address from DHCP server.

Example Your Product# release dhcp vlan 1

Related Command(s)

- `no switchport` – Configures the port as a router port.
- `ip address - rarp/dhcp` - Configures the current VLAN / OOB interface to dynamically acquire an IP address from the RARP / DHCP server.
- `show ip dhcp client stats` - Displays the DHCP client statistics information for interfaces that are configured to acquire IP address dynamically from the DHCP server.
- `show ip interfaces` - Displays the IP interface configuration for all interfaces available in the switch.

renew dhcp

Command Objective This command immediately renews the DHCP lease for the interface specified. The current lease acquired by the specified interface is manually renewed or else a new DHCP lease is acquired for interface whose lease is terminated. The DHCP lease is automatically renewed, once the lease expires.

Syntax **renew dhcp { vlan <vlan-id (1-4094)> | <interface-type> <interface-id> }**

Parameter Description

- `vlan <vlan-id (1-4094)>` - Renews the DHCP lease for the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.

- `vlanMgmt` - Renews the DHCP lease for the management vlan interface.
- `<interface-type>` - Renews the DHCP lease for the specified type of interface. The interface can be:
  - `qx-ethernet`– A version of LAN standard architecture that supports data transfer up to 40 GIgabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Renews the DHCP lease for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided for interface type port-channel. For example: 1 represents port-channel ID.

Mode Privileged EXEC Mode

Note: This command executes successfully only if the VLAN interfaces and router ports are in BOUND state (that is, IP address is dynamically acquired from DHCP server and an active lease is bound to the interface). The port should have been configured as router port for dynamically acquiring an IP address from DHCP server.

Example Your Product# renew dhcp vlan 1

Related Command(s)

- `no switchport` – Configures the port as a router port.
- `ip address – rarp/dhcp` - Configures the current VLAN / OOB interface to dynamically acquire an IP address from the RARP / DHCP server.
- `show ip dhcp client stats` - Displays the DHCP client statistics information for interfaces that are configured to acquire IP address dynamically from the DHCP server.
- `show ip interface` - Displays the IP interface configuration for all interfaces available in the switch.

show ip dhcp client stats

Command Objective This command displays the DHCP client statistics information for interfaces that are configured to acquire IP address dynamically from the DHCP server.

The statistics information contains interface name, IP address assigned by DHCP server, DHCP lease details, details regarding number of DHCPDISCOVER, DHCPREQUEST, DHCPDECLINE, DHCPRELEASE and DHCPINFORM packets received and number of DHCPOFFER packets sent from the DHCP client.

Syntax **show ip dhcp client stats**

Mode Privileged EXEC Mode

Example

```
Your Product# show ip dhcp client stats
Dhcp Client Statistics
----------------------------------------
Interface                     : vlan1
Client IP Address             : 12.0.0.21
Client Lease Time             :  3600
Client  Remain  Lease  Time   :  3569
Message Statistics
----------------------------------
DHCP                   DISCOVER              :    1
DHCP                   REQUEST               :    1
DHCP                   DECLINE               :    0
DHCP                   RELEASE               :    0
DHCP                   INFORM                :    0
DHCP                   OFFER                 :    1
```

Related Command(s)

- `ip address – rarp/dhcp` - Configures the current VLAN / OOB interface to dynamically acquire an IP address from the RARP / DHCP server.
- `release dhcp` - Releases, on the specified interface, the DHCP lease obtained for an IP address from a DHCP server.
- `renew dhcp` - Renews the DHCP lease for the interface specified.

ip dhcp client discovery timer

Command Objective This command configures DHCP Client Discovery timer, which denotes the time to wait between discovery messages sent by the DHCP client. This value ranges between 1 and 9.

The no form of the command resets DHCP Client discovery timer with its default values.

Syntax **ip dhcp client discovery timer <integer (1-9)>**

no ip dhcp client discovery timer

Mode Privileged EXEC Mode

Default

- If dhcp fast mode is enabled , the default DHCP Client Discovery timer is 5.
- If dhcp fast mode is disabled , the default DHCP Client Discovery timer is 15.

Example Your Product# ip dhcp client discovery timer 8

Related Command(s)

- `show ip dhcp client fast-access` - Displays DHCP fast access details
- `ip dhcp client fast-access` - Enables DHCP fast access Mode

ip dhcp client idle timer

Command Objective This command configures DHCP Client idle timer which specifies the time to wait after four unsuccessful DHCP client discovery messages. This value ranges between 1 and 30.

The no form of the command resets the DHCP Client idle timer with the default values.

Syntax **ip dhcp client idle timer <integer (1-30)>**

no ip dhcp client idle timer

Mode Privileged EXEC Mode

Default

- If dhcp fast mode is enabled, the default DHCP Client Idle timer is 1.
- If dhcp fast mode is disabled, the default DHCP Client Idle timer is 180.

Example

```
Your Product# ip dhcp client idle timer 8
```

Related Command(s)

- `show ip dhcp client fast-access` - Displays DHCP fast access details
- `ip dhcp client fast-access` - Enables DHCP fast access Mode

ip dhcp client arp-check timer

Command Objective This command configures DHCP client retransmission timeout between arp messages. This value ranges between 1 and 20.

The no form of the command resets DHCP Client arp timer with the default values.

Syntax **ip dhcp client arp-check timer <integer (1-20)>**

no ip dhcp client arp-check timer

Mode Privileged EXEC Mode

Default

- If dhcp fast mode is enabled, the default DHCP Client arp-check timer is 1.
- If dhcp fast mode is disabled, the default DHCP Client arp-check timer is 3.

Example `Your Product# ip dhcp client arp-check timer 8`

Related Command(s)

- `ip dhcp client fast-access` - Enables DHCP fast access Mode
- `show ip dhcp client fast-access` - Displays DHCP fast access details

ip dhcp client fast-access

Command Objective This command enables DHCP fast access Mode.

If fast access mode is enabled, time to wait between discovery messages i.e. discovery timeout and time to wait after four unsuccessful discovery will be user configurable and the default value for discovery timeout is 5 seconds and for the null state timeout is 1 second.

The no form of the command disables DHCP Client fast access mode. If the mode is disabled, default value for discovery timeout and null state timeout will be 15 seconds and 180 seconds respectively. The timeout values cannot be changed under disable mode.

Syntax **ip dhcp client fast-access**

no ip dhcp client fast-access

Mode Privileged EXEC Mode

Example `Your Product# ip dhcp client fast-access`

Related Command(s)

- `ip dhcp client discovery timer` – Configures DHCP Client Discovery timer,
- `ip dhcp client idle timer` – Configures DHCP Client idle timer
- `ip dhcp client arp-check timer` - Configures DHCP client retransmission timeout between arp messages
- `show ip dhcp client fast-access` - Displays DHCP fast access details

ip dhcp client client-id

Command Objective This command sets unique identifier to dhcp client identifier. This command advertises the client-id in the DHCP control packets.

The no form of the command resets the dhcp client identifier

Syntax **ip dhcp client client-id {<interface-type> <interface-id> | vlan <vlan-id (1-4094)> | port-channel <port-channel-id (1-65535)> | tunnel <tunnel-id (0-128)> | loopback <interface-id (0-100)> | ascii <string> | hex <string> }**

no ip dhcp client client-id

Parameter Description

- `<interface-type>` - Configures interface type for the DHCP client-id for the specified type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-id>` - Configures interface id for the DHCP client-id for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1.Only port-channel ID is provided for interface type port-channel. For example: 1 represents port-channel ID.
- `<vlan-id (1-4094)>` - Configures DHCP client-id for the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.
- `<port-channel-id (1-65535)>` - Configures the port to be used by the host to configure the router. This value ranges between 1 and 65535. The port channel identifier can be created or the port channel related configuration done only if the LA feature is enabled in the switch.
- `tunnel<tunnel-id (0-128)>` - Configures the tunnel identifier. This value ranges between 0 and 128
- `loopback <interface-id (0-100)>` - Configures the loopback identifier. The value ranges between 0 and 100
- `ascii <string>`- Configures the client-id in ascii format. The client-id is given as a string.
- `hex <string>`- Configures the client-id in hexa decimal format. The input type is a string.

Mode Interface Configuration Mode (Vlan)

Example

```
Your Product (config-if)# ip dhcp client client-id gigabitethernet 0/1
```

Related Command(s) `show ip dhcp client client-id`- Displays DHCP client client identifier.

ip dhcp client request

Command Objective This command sets the dhcp option type to request the server. This is required to send DHCP request to get the tftp server name and Boot file name.

The no form of the command resets the dhcp option type to request the server.

Syntax **ip dhcp client request { tftp-server-name | boot-file-name}**

no ip dhcp client request {tftp-server-name | boot-file- name}

Parameter Description

- `tftp-server-name` - Sends the DHCP requests to get the TFTP server's domain name.
- `boot-file-name` - Sends the DHCP requests to get the boot File Name.

Mode Interface Configuration Mode (Vlan)

This command executes successfully only if the VLAN interfaces and router ports are in BOUND state (that is, IP address is dynamically acquired from DHCP server and an active lease is bound to the interface).

Example `Your Product (config-if)# ip dhcp client request tftp- server-name`

Related Command(s) `show ip dhcp client option` – Displays DHCP client options set by Server

show ip dhcp client fast-access

Command Objective This command displays DHCP fast access information such as Fast Access Mode status, Dhcp Client Fast Access DiscoverTimeOut, Dhcp Client Fast Access NullStateTimeOut, Dhcp Client Fast Access Arp Check TimeOut values.

Syntax **show ip dhcp client fast-access**

Mode Privileged EXEC Mode

Example `Your Product# show ip dhcp client fast-access le`

Related Command(s)

- `ip dhcp client discovery timer` – Configures DHCP Client Discovery timer,
- `ip dhcp client idle timer` – Configures DHCP Client idle timer
- `ip dhcp client arp-check timer` - Configures DHCP client retransmission timeout between arp messages
- `ip dhcp fast-access` - Enables DHCP fast access Mode

show ip dhcp client option

Command Objective This command displays DHCP client options set by Server which provides the details like interface, interface type, length and value.

Syntax **show ip dhcp client option**

Mode Privileged EXEC Mode

Example

```
Your Product# show ip dhcp client option
Dhcp Client Options
Interface                Type      Len    Value
```

```
---------                ----     ---    ------
vlan1                    66
```

Related Command(s) `ip dhcp client request` – Sets the dhcp option type to request the server

show ip dhcp client client-id

Command Objective This command displays the unique identifier to DHCP client.

Syntax **show ip dhcp client client-id**

Mode Privileged EXEC Mode

Example Your Product# show ip dhcp client client-id

Related Command(s)

- `ip dhcp client client-id` – Sets unique identifier to dhcp client
- `ip dhcp client request` - Sets the dhcp option type to request the server

23.2 DHCP Relay

DHCP relay agent is a host or an IP router that allows the DHCP client and DHCP server in different subnets to communicate with each other, so that the DHCP client can obtain its configuration information while booting. The relay agent receives packets from the client, inserts information such as network details, and forwards the modified packets to the server. The server identifies the client's network from the received packets, allocates the IP address accordingly, and sends reply to the relay. The relay strips the information inserted by the server and broadcasts the packets to the client's network.

The list of CLI commands for the configuration of DHCP Relay is as follows:

- service dhcp-relay
- ip dhcp server
- ip helper-address
- ip dhcp relay information option
- ip dhcp relay circuit-id option
- ip dhcp relay circuit id
- ip dhcp relay remote id
- debug ip dhcp relay
- show ip dhcp relay information
- show dhcp server

service dhcp-relay

Command Objective This command enables the DHCP relay agent in the switch. DHCP relay agent relays DHCP messages between DHCP client and DHCP server located in different subnets.

The no form of the command disables the DHCP relay agent.

Syntax **service dhcp-relay**

no service dhcp-relay

Mode Global Configuration Mode

Default DHCP relay agent is disabled (that is, the switch acts as a DHCP client)

Note: The DHCP relay agent can be enabled in the switch, only if the DHCP server is disabled in the switch.

Example

```
Your product(config)# service dhcp-relay
```

Related Command(s)

- no service dhcp-service – Disables the DHCP server.
- show ip dhcp relay information - Displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured.

ip dhcp server

Command Objective This command adds the configured IP address to the IP address list created forthe DHCP server. The switches or systems having these IP addresses represent the DHCP servers to which the DHCP relay agent can forward the packets that are received from DHCP clients.

The DHCP relay agent broadcasts the received packets to entire network except the network from which the packets are received, if the DHCP server list is empty (that is IP address is configured as 0.0.0.0).

The no form of the command deletes the mentioned IP address from the IP address list.

Note: The IP address list can contain only 5 IP addresses (that is, only a maximum of 5 DHCP servers can be listed).

Syntax **ip dhcp server <ip address>**

no ip dhcp server <ip address>

Mode Global Configuration Mode

Default DHCP server list

Example

```
Your product(config)# ip dhcp server 12.0.0.1
```

Related Command(s)

- `show ip dhcp relay information` - Displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured.
- `show dhcp server` - Displays the DHCP servers' IP addresses

ip helper-address

Command Objective This command sets the IP address of the DHCP server. The relay agent starts forwarding the packets (that is, UDP broadcasts including BOOTP) from the client to the specified DHCP server. This command allows to add more than one DHCP server.

This command is a complete standardized implementation of the existing command ip dhcp server and operates similar to that of the command ip dhcp server. This command also explicitly enables the DHCP relay and disables the DHCP server.

Syntax **ip helper-address <ip address>**

Mode Interface Configuration Mode (Physical)

Default The IP address is 0.0.0.0 and the status of the DHCP Relay Servers only is disabled.

Note: The relay agent will start forwarding the packets from the client to a specific DHCP server only when the relay agent is in the enabled state.

Example

```
Your product(config-if)# ip helper-address 12.0.0.1
```

Related Command(s)

- `show ip dhcp relay information` - Displays the DHCP relay information
- `show dhcp server` - Displays the DHCP Server information

ip dhcp relay information option

Command Objective This command enables the DHCP relay agent to perform processing related to DHCP relay agent information option.

The options contain a sub-option for agent circuit ID details and another sub- option for agent remote ID details. The processing involves:

- Insertion of DHCP relay information option in DHCP request messages forwarded to a DHCP server from a DHCP client.
- Examining / removing of DHCP relay information option from DHCP response messages forwarded to the DHCP client from the DHCP server.

The no form of the command disables the processing related to DHCP relay agent information option.

Syntax **ip dhcp relay information option**

no ip dhcp relay information option

Mode Global Configuration Mode

Note: This command can also be executed in the VLAN Interface Configuration Mode for a code base using industry standard commands.

Default Processing related to DHCP relay agent information option is disabled.

Example `Your product(config)# ip dhcp relay information option`

Related Command(s)

- ip dhcp relay circuit-id option – Defines the type of information to be present in circuit ID sub-option that is used in the DHCP relay agent information option.
- show ip dhcp relay information - Displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured.

ip dhcp relay circuit-id option

Command Objective This command defines the type of information to be present in circuit ID sub-option that is used in the DHCP relay agent information option.

Syntax **ip dhcp relay circuit-id option [router-index] [vlanid] [recv-port]**

Parameter Description

- `router-index` - Adds information related to router interface indexes in the circuit ID sub-option.
- `vlanid` - Adds information related to VLAN IDs in the circuit ID sub-option.
- `recv-port` - Adds information related to physical interfaces or LAG ports in the circuit ID sub-option

Mode Global Configuration Mode

Default router-index

Note: The type of information to be present in the circuit ID sub-option can be configured, only if the DHCP relay agent is enabled to perform processing related to DHCP relay agent information option.

Example `Your product(config)# ip dhcp relay circuit-id option vlanid`

Related Command(s)

- `ip dhcp relay information option` - Enables the DHCP relay agent to perform processing related to DHCP relay agent information option.
- `show ip dhcp relay information` - Displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured.

ip dhcp relay circuit id

Command Objective This command configures circuit ID value for an interface.

The circuit ID uniquely identifies a circuit over which the incoming DHCP packet is received. In DHCP relay, it is used to identify the correct circuit over which the DHCP responses should be relayed.

The configured circuit ID is used in the DHCP relay agent information option to inform the DHCP server about the interface from which DHCP packet is received. The circuit ID is unique for the interfaces and ranges from 1 to 2147483647.

The minimum value depends upon the number of interfaces that can be created. For example, if a total of 160 interfaces are allowed to be created in the switch, then the circuit ID value range starts from 161 only. The interfaces include all physical interfaces, port channels and logical L3 interfaces.

The no form of the command deletes the circuit ID configuration for the interface (that is, the circuit ID is configured as 0).

Syntax **ip dhcp relay circuit-id <circuit-id>**

no ip dhcp relay circuit-id

Mode Interface Configuration Mode (Vlan / Router Ports)

Note: This command is available only for the VLAN interfaces and ports that are configured as router ports.

Example

```
Your product(config-if)# ip dhcp relay circuit-id 1
```

Related Command(s)

- `no switchport` – Configures the port as a router port.
- `show ip dhcp relay information` - Displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured.

ip dhcp relay remote id

Command Objective This command configures remote ID value for an interface.

The configured remote ID is used to inform the DHCP client about the remote circuit to which the DHCP packets should be forwarded from the interface. The remote ID is globally unique and an octet string of maximum size of 32. The remote ID should not be same as that of the default value.

The no form of the command deletes the remote ID configuration for the interface (that is, the remote ID is set with a string of length zero).

Syntax **ip dhcp relay remote-id <remote-id name>**

no ip dhcp relay remote-id

Mode Interface Configuration Mode (Vlan / Router Ports)

Default XYZ. This value is internally assigned.

Note: This command is available only for the VLAN interfaces and ports that are configured as router ports.

Example `Your product(config-if)# ip dhcp relay remote-id SMIS`

Related Command(s)

- `no switchport` – Configures the port as a router port.
- `show ip dhcp relay information` - Displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured.

debug ip dhcp relay

Command Objective This command enables the tracking of the DHCP relay module operations as per the configured debug levels. The debug statements are generated for the configured trace level.

The no form of the command disables the tracking of the DHCP relay module operations. The debug statements are not generated for the configured trace levels.

Syntax **debug ip dhcp relay {all | errors}**

no debug ip dhcp relay {all | errors}

Parameter Description

- `all` - Generates debug statements for all kind of failure traces.
- `errors` - Generates debug statements for trace error code debug messages. These messages are generated for all error events generated.

Mode Privileged EXEC Mode

Default Tracking of the DHCP relay module operation is disabled.

Example `Your product# debug ip dhcp relay all`

Related Command(s)

- `show ip dhcp relay information` - Displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured.
- `show debugging` - Displays state of each debugging option

show ip dhcp relay information

Command Objective This command displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured.

The information contains status of the DHCP relay, DHCP server IP addresses, status of relay information option, configured debug level and statistics details regarding number of packets affected by relay information option, circuit ID suboption, remote ID suboption, and subnet mask sub option.

Syntax **show ip dhcp relay information [vlan <vlan-id>]**

Parameter Description `vlan<vlan-id>` - Displays the DHCP relay agent configuration information for the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094.

Mode Privileged EXEC Mode

Example

```
Your product# show ip dhcp relay information

Dhcp Relay                        : Enabled
Dhcp Relay Servers only           : Enabled
DHCP server 1                     : 12.0.0.1
Dhcp Relay RAI option             : Enabled
Default Circuit Id information    :  router-index
Debug Level                                            : 0x1
No of Packets inserted RAI option                      :  0
No of Packets inserted circuit ID suboption         : 0 No
of Packets inserted remote ID suboption                :  0
No of Packets inserted subnet mask suboption        : 0 No
of Packets dropped                                     : 0
No  of  Packets  which  did  not  inserted  RAI  option  :  0
Interface vlan1
Circuit ID : 162
Remote ID : 45
```

Related Command(s)

- `service dhcp-relay` - Enables the DHCP relay agent in the switch.
- `ip dhcp server` - Adds the configured IP address to the IP address list created for the DHCP server.
- `ip dhcp relay information option` - Enables the DHCP relay agent to perform processing related to DHCP relay agent information option.
- `ip dhcp relay circuit-id option` - Defines the type of information to be present in circuit ID sub-option that is used in the DHCP relay agent information option.
- `ip dhcp relay circuit-id`– Configures circuit ID value for an interface.
- `ip dhcp relay remote-id`– Configures remote ID value for an interface.
- `debug ip dhcp relay` - Enables the tracking of the DHCP relay module operations as per the configured debug levels

show dhcp server

Command Objective This command displays the DHCP servers' IP addresses. These addresses denote the PCs or switches that can act as a DHCP server.

Syntax **show dhcp server**

Mode Privileged EXEC Mode

Example

```
Your product# show dhcp server
DHCP server: 40.0.0.4
```

Related Command(s) `ip dhcp server`- Adds the configured IP address to the IP address list created for the DHCP server.

23.3 DHCP Server

DHCP server is responsible for dynamically assigning unique IP address and other configuration parameters such as gateway, to interfaces of a DHCP client. The IP address is leased to the interface only for a particular time period as mentioned in the DHCP lease. The interface should renew the DHCP lease once it expires. The DHCP server contains a pool of IP address from which one address is assigned to the interface.

The list of CLI commands for the configuration of DHCP Server is as follows:

- service dhcp-server
- service dhcp
- ip dhcp pool
- ip dhcp next-server
- ip dhcp bootfile
- bootfile config-file
- ip dhcp
- ip dhcp option
- network
- excluded-address
- ip dhcp excluded-address
- domain-name
- dns-server
- netbios-name-server
- netbios-node-type
- default-router
- option
- lease
- utilization threshold
- host hardware-type
- debug ip dhcp server
- show ip dhcp server information
- show ip dhcp server pools
- show ip dhcp server binding

- show ip dhcp server statistics

service dhcp-server

Command Objective This command enables the DHCP server in the switch (that is, switch acts as DHCP server). The DHCP server assigns unique IP address and other configuration parameters such as gateway, to interfaces of a DHCP client.

The no form of the command disables the DHCP server in the switch.

Syntax **service dhcp-server**

no service dhcp-server

Mode Global Configuration Mode

Default DHCP server is disabled (that is, the switch acts as a DHCP client)

Note: The DHCP server can be enabled in the switch, only if the DHCP relay agent is disabled in the switch.

Example

```
Your product (config)# service dhcp-server
```

Related Command(s)

- `no service dhcp-relay` - Disables the DHCP relay agent in the switch.
- `show ip dhcp server information` - Displays the DHCP server configuration information.
- `show ip dhcp server binding` - Displays the DHCP server binding information
- `show ip dhcp server statistics` - Displays various DHCP server statistics related information such as number of DHCPDECLINE messages received, DHCPOFFER messages sent and so on.

service dhcp

Command Objective This command enables the DHCP server in the switch and relay agent features on router which assigns unique IP address andother configuration parameters to interfaces of a DHCP client.

The no form of this command disables the DHCP Server.

This command is a complete standardized implementation of the existing command and operates similar to that of the command service dhcp-server.

Syntax **service dhcp**

no service dhcp

Mode Global Configuration Mode

Default DHCP Server is disabled.

Note: The DHCP server can be enabled in the switch, only if the DHCP relay agent is disabled in the switch.

Example `Your product(config)# service dhcp`

Related Command(s)

- `no service dhcp-relay` - Disables the DHCP relay agent in the switch.
- `show ip dhcp server information` - Displays the DHCP server configuration information.
- `show ip dhcp server binding` - Displays the DHCP server binding information
- `show ip dhcp server statistics` - Displays various DHCP server statistics related information such as number of DHCPDECLINE messages received, DHCPOFFER messages sent and so on.

ip dhcp pool

Command Objective This command creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.

The address pool has a range of IP addresses that can be assigned to the DHCP client and also information about client configuration parameters such as domain name. The pool created is identified with a unique ID whose value ranges between 1 and 2147483647.

The no form of the command deletes the existing DHCP server address pool.

Syntax **ip dhcp pool <index (1-2147483647)>**

no ip dhcp pool <index (1-2147483647)>

Mode Global Configuration Mode

Example `Your product (config)# ip dhcp pool 1`

Related Command(s)

- `network` - Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- `excluded-address` - Creates an excluded pool that defines a range of IP addresses which needs to be excluded from the created subnet pool.
- `domain-name` - Configures the domain name option for the corresponding DHCP server address pool.
- `dns-server` - Configures the IP address of a DNS server for the corresponding DHCP server address pool.
- `netbios-name-server` - Configures the IP address of a NetBIOS and WINS name server that is available to Microsoft DHCP clients.
- `netbios-node-type` - Configures the NetBIOS node type for Microsoft DHCP clients, for the corresponding DHCP server address pool.
- `default-router` - Configures the IP address of a default router to which a DHCP client should send

packets after booting, for the corresponding DHCP server address pool.

- `option` - Configures, for the corresponding DHCP server address pool, the various available DHCP server options with the corresponding specific values.
- `lease` - Configures, for the corresponding DHCP server, the DHCP lease period for an IP address that is assigned from a DHCP server to a DHCP client.
- `utilization threshold` - Configures pool utilization threshold value (in percentage) for the corresponding DHCP server address pool.
- `host hardware-type` - Configures host hardware type and its DHCP option with specific values for the corresponding DHCP server address pool.
- `show ip dhcp server pools` - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.
- `show ip dhcp server statistics` - Displays various DHCP server statistics related information such as number of DHCPDECLINE messages received, DHCPOFFER messages sent and so on.

ip dhcp next-server

Command Objective This command sets the IP address of the boot server (that is, TFTP server) from which the initial boot file is to be loaded in a DHCP client. This boot server acts as a secondary server.

The no form of the command deletes the boot server details and resets to its default value.

The DHCP server is used as the boot server, if no TFTP server is configured as the boot server.

Syntax **ip dhcp next-server <ip address>**

no ip dhcp next-server

Mode Global Configuration Mode

Default 0.0.0.0 (No boot server is defined. DHCP server is used as the boot server)

Example

```
Your product (config)# ip dhcp next-server 12.0.0.1
```

Related Command(s)

- `ip dhcp bootfile` - Configures the name of the initial boot file to be loaded in a DHCP client.
- `show ip dhcp server information` - Displays the DHCP server configuration information

ip dhcp bootfile

Command Objective This command configures the name of the initial boot file to be loaded in a DHCP client. The file name is a string whose maximum size is 63. The boot file contains the boot image that is used as the operating system for the DHCP client.

The no form of the command deletes the boot file name (that is, no file is specified as the initial boot file).

Syntax **ip dhcp bootfile <bootfile (63)>**

no ip dhcp bootfile

Mode Global Configuration Mode

Example `Your product (config)# ip dhcp bootfile 53`

Related Command(s)

- `ip dhcp next-server` - Sets the IP address of the boot server (that is, TFTP server) from which the initial boot file is to be loaded.
- `show ip dhcp server information` - Displays the DHCP server configuration information

bootfile config-file

Command Objective This command defines the name of the boot image file that the DHCP client should download during auto install process. The DHCP server passes this file name to the DHCP client. The maximum size of the string is 63.

The no form of this command deletes the specified boot file name and assigns the value of boot file name as None (that is, no file is set as boot image file).

This command is a complete standardized implementation of the existing command and operates similar to that of the command ip dhcp bootfile.

Syntax **bootfile config-file <bootfile (63)>**

no bootfile config-file

Mode Global Configuration Mode

Default None (Null terminated string)

Example Your product(config)# bootfile config-file boot.img

Related Command(s) `show ip dhcp server information` - Displays the DHCP Server information

ip dhcp

Command Objective This command enables ICMP echo mechanism or configures offer-reuse timeout for the DHCP server. These parameters are used to control the allocation of IP address to a DHCP client.

The no form of the command disables ICMP echo mechanism, resets server offer-reuse time to its default value or removes a bind entry from a server binding table.

Syntax **ip dhcp { ping packets [<count(0-10)>] | server offer- reuse <timeout (1-120)> }**

no ip dhcp { ping packets | server offer-reuse | binding <ip address> }

Parameter Description

- `ping packets` - Enables / disables ICMP echo mechanism. This mechanism allows the DHCP server to verify the availability of an IP address before assigning it to a DHCP client. DHCP server sends ping packets to the IP address that is intended to be assigned for the DHCP client. If the ping operation fails, DHCP server assumes that the address is not in use and assigns the address to the requesting DHCP client
- `<count(0-10)>` - Configures the number of ping packets to be sent from the DHCP server to the pool address before assigning the address to a requesting client. The pinging of pool addresses is disabled, if the count value is set as 0. This value ranges from 0 to 10. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
- `server offer-reuse` - Configures the amount of time (in seconds), the DHCP server entity should wait for the DHCP REQUEST from the DHCP client before reusing the lease offer for other DHCP client. This value ranges between 1 and 120 seconds.
- `binding` - Deletes the specified IP address entry from the server binding table. This frees the IP address allocated to a DHCP client, so that the IP address can be allocated for another DHCP client.

Mode Global Configuration Mode

Default

- `ping packets` - ICMP echo mechanism feature is disabled.
- `server offer-reuse` - 5

Example

```
Your product (config)# ip dhcp ping packets
```

Related Command(s)

- `show ip dhcp server information` - Displays the DHCP server configuration information.
- `show ip dhcp server binding` - Displays the DHCP server binding information.
- `show ip dhcp server statistics` - Displays various DHCP server statistics related information such as number of DHCPDECLINE messages received, DHCPOFFER messages sent and so on.

ip dhcp option

Command Objective This command sets the DHCP Server options. This command globally configures the various available DHCP server options with the corresponding specific values. These values can be an ASCII string, hexadecimal string or IP address. These global options are applicable for all DHCP server address pools.

The no form of the command deletes the existing DHCP server option.

Syntax **ip dhcp option <code (1-2147483647)> { ascii <string> | hex <Hex String> | ip <address> }**

no ip dhcp option <code (1-2147483647)>

Parameter Description

- `<code (1-2147483647)>` - Configures the unique DHCP option code that represents a specific DHCP option used in a DHCP OFFER message in response to a DHCP DISCOVER message. This value ranges from 1 to 2147483647.
- `ascii<string>` - Configures the ASCII value to be set for the corresponding option code that accepts ASCII string. This value is a character string that should contain only characters from NVT ASCII character set.
- `hex<Hex String>` - Configures the hexadecimal value to be set for the corresponding option code that accepts hexadecimal string.
- `ip<address>` - Configures the unicast IP address to be set for the corresponding option code that accepts IP address.

Mode Global Configuration Mode

Example Your product(config)# ip dhcp option 19 hex d

Related Command(s) `show ip dhcp server pools` - Displays global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

network

Command Objective This command creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.

The no form of the command deletes the created subnet pool.

Syntax **network <start- IP> [{ <mask> | / <prefix-length (1-31)>}] [end ip]**

no network

Parameter Description

- `<start-IP>` - Configures the IP subnet address for the DHCP pool. The addresses within the specified network subnet are assigned to the DHCP client, if no restriction is applied. For example: The value is configured as 20.0.0.0, then any one of the address within the range from 20.0.0.1 to 20.255.255.254 can be assigned to the DHCP client if no other limitations such as end IP address, are set. This value should be unique (that is, one subnet address can be assigned only for one DHCP address pool).
- `<mask>` - Configures the subnet mask for the network IP address. This is a 32-bit number which is used to divide the IP address into network address and host address. This value is used to automatically calculate the end IP address for the pool. For example: The value 254.0.0.0 represents that the end IP address is 21.255.255.254, if the network subnet is set as 20.0.0.0.
- `<prefix-length (1-31)>` - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value should be preceded by a slash (/) with space before and after the slash. This value is used to automatically calculate the end IP address for the pool and set the mask for the subnet. For example: value 20.0.0.0 / 6 represents that the end ip address is 23.255.255.254 and the mask is 252.0.0.0.

- `<end ip>` - Configures the end IP address for the network IP subnet set for theDHCP address pool. This value restricts the IP addresses that can be assigned to the DHCP client. This value is used to manually set the end IP address. This value overrides the end IP address calculated automatically using the mask or prefix-length.

Mode DHCP Pool Configuration Mode

Default

- `mask` - 255.0.0.0
- `end ip` - Represents the last possible subnet address. For example: If network subnet address is mentioned as 20.0.0.0, then end IP address would be 20.255.255.254.

Example

```
Your product(dhcp-config)# network 20.0.0.0 255.0.0.0
20.0.0.50
```

Related Command(s)

- `ip dhcp pool` - Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- `excluded-address` - Creates an excluded pool that defines a range of IP addresses which needs to be excluded from the created subnet pool.
- `domain-name` - Configures the domain name option for the corresponding DHCP server address pool.
- `dns-server` - Configures the IP address of a DNS server for the corresponding DHCP server address pool.
- `netbios-name-server` - Configures the IP address of a NetBIOS and WINS name server that is available to Microsoft DHCP clients.
- `netbios-node-type` - Configures the NetBIOS node type for Microsoft DHCP clients, for the corresponding DHCP server address pool.
- `netbios-node-type` - Configures the IP address of a default router to which a DHCP client should send packets after booting, for the corresponding DHCP server address pool.
- `option` - Configures, for the corresponding DHCP server address pool, the various available DHCP server options with the corresponding specific values.
- `Lease` - Configures, for the corresponding DHCP server, the DHCP lease period for an IP address that is assigned from a DHCP server to a DHCP client.
- `utilization threshold` - Configures pool utilization threshold value (in percentage) for the corresponding DHCP server address pool.
- `show ip dhcp server pools` - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

excluded-address

Command Objective This command creates an excluded pool that defines a range of IP addresses which needs to be excluded from the created subnet pool. That is, the IP addresses in this range including start and end IP address of the excluded pool are not assigned to any DHCP client.

The no form of the command deletes the created excluded pool. The same start IP address and end IP address of the already created excluded pool should be provided while executing the no form of the command.

Syntax **excluded-address <low-address> <high-address>**

no excluded-address <low-address> [<high-address>]

Parameter Description

- `<low-address>` - Sets the start IP address for an excluded pool. This address denotes the first IP address of a range of IP addresses which needs to be excluded from the created subnet pool. This IP address should be:
  - lower than the end IP address, and
  - in the same network of the subnet pool's start IP address.
- `<high-address>` - Sets the end IP address for an excluded pool. This address denotes the last IP address of a range of IP addresses which needs to be excluded from the created subnet pool. This IP address should be:
  - high than the start IP address, and
  - within or equal to the subnet pool's end IP address.

Mode DHCP Pool Configuration Mode

Note: This command is executed successfully, only if a subnet pool is already created for the DHCP address pool.

Example

```
Your product(dhcp-config)# excluded-address 20.0.0.1
20.0.0.30
```

Related Command(s)

- `ip dhcp pool` - Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- `network` - Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- `show ip dhcp server pools` - Displays the global DHCP option configuration for all DHCP server address pools.

ip dhcp excluded-address

Command Objective This command creates an excluded pool to prevent DHCP server from assigning certain addresses to DHCP clients. The no form of the command deletes the excluded pool.

This command is a complete standardized implementation of the existing command and operates similar to that of the command excluded-address. This command is used to exclude a single IP address or a range of IP addresses.

Syntax **ip dhcp excluded-address <low-address> [<high-address>]**

no ip dhcp excluded-address <low-address> [high-address]

Parameter Description

- `low-address` - Configures the excluded IP address, or first IP address in an excluded address range
- `high-address` - Configures the last IP address in the excluded address range

Mode Global Configuration Mode

Note: Subnet pool should have been created before creating an excluded pool. This excluded pool should be within the range of the created subnet pool.

For example, the excluded pool 20.0.0.20 – 20.0.0.30 created using this command is within the already created subnet pool 20.0.0.0 – 20.0.0.100.

Example

```
Your product(config)# ip dhcp excluded-address 20.0.0.20
20.0.0.30
```

Related Command(s)

- `ip dhcp pool` - Creates a DHCP Server address pool and places the user in the DHCP pool configuration mode
- `network` - Sets the network IP and mask in DHCP Server configuration parameters
- `service dhcp-server` - Enables the DHCP Server
- `show ip dhcp server information` - Displays the server information
- `show ip dhcp server pools` - Displays the DHCP Server pools
- `show ip dhcp server binding` - Displays the DHCP Server binding information
- `show ip dhcp server statistics` - Displays the DHCP Server statistics

domain-name

Command Objective This command configures the domain name option for the corresponding DHCP server address pool. A DHCP client uses this domain name while resolving host names through a domain name system. The DHCP option code is 15. This value is a string whose maximum size is 63.

The no form of the command deletes the domain name option configuration for the DHCP server address pool. The domain name option configuration is deleted, if the no form of the network command is executed successfully.

Syntax **domain-name <domain (63)>**

no domain-name

Mode DHCP Pool Configuration Mode

Note: The domain name configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Example

```
Your product(dhcp-config)# domain-name Aricent
```

Related Command(s)

- `ip dhcp pool` - Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- `network` - Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- `show ip dhcp server pools` - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

dns-server

Command Objective This command configures the IP address of a DNS server for the corresponding DHCP server address pool. The client correlates the DNS IP address with the host name. The DNS server is used to translate domain names and hostnames into corresponding IP addresses.

The no form of the command deletes the DNS server IP address option configuration for the DHCP server address pool. The DNS server IP address option configuration is deleted, if the no form of the network command is executed successfully.

Syntax **dns-server <ip address>**

no dns-server

Mode DHCP Pool Configuration Mode

Note: The DNS server IP address configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Example

```
Your product(dhcp-config)# dns-server 20.0.0.1
```

Related Command(s)

- `ip dhcp pool` - Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- `network` - Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- `show ip dhcp server pools` - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

netbios-name-server

Command Objective This command configures, for the corresponding DHCP server address pool, the IP address of a NetBIOS (Network Basic Input / Output System) and WINS (Windows Internet Naming Service) name server that is available to Microsoft DHCP clients.

The no form of the command deletes the NetBIOS and WINS name server IP address configuration for the DHCP server address pool. The NetBIOS WINS name server option configuration is deleted, if the no form of the network command is executed successfully.

The NetBIOS name server provides the following three distinct services:

1. Name service for name registration and resolution
2. Session service for connection oriented communication
3. Datagram distribution service for connectionless communication

Syntax **netbios-name-server <ip address>**

no netbios-name-server

Mode DHCP Pool Configuration Mode

Note: The NetBIOS WINS name server configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Example

```
Your product(dhcp-config)# netbios-name-server 20.0.0.3
```

Related Command(s)

- `ip dhcp pool` - Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- `network` - Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- `show ip dhco server pools` - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

netbios-node-type

Command Objective This command configures the NetBIOS node type for Microsoft DHCP clients, for the corresponding DHCP server address pool. The node type denotes the method used to register and resolve NetBIOS names to IP addresses.

The no form of the command deletes the NetBIOS node type option configuration for the DHCP server address pool.

Syntax **netbios-node-type { <0-FF> | b-node | h-node | m-node | p- node }**

no netbios-node-type

Parameter Description

- `<0-FF>` - Allows NetBIOS over TCP/IP clients. This value ranges from 0 to 255.
- `b-node` - Configures the DHCP server address pool to broadcast IP messages for registering and resolving NetBIOS names to IP addresses. The node type value is set as 1.
- `h-node` - Configures the DHCP server address pool to initially query name server and subsequently broadcast IP messages for registering and resolving NetBIOS names to IP addresses. The node type value is set as 8. This node type is the best option for all conditions.
- `m-node` - Configures the DHCP server address pool to initially broadcast IP message and then query name server for registering and resolving NetBIOS names to IP addresses. The node type value is set as 4.
- `p-node` - Configures the DHCP server address pool to have point-to-point communication with a NetBIOS name server for registering and resolving NetBIOS names to IP addresses. The node type value is set as 2.

Mode DHCP Pool Configuration Mode

Note: The NetBIOS node type configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Example

```
Your product(dhcp-config)# netbios-node-type h-node
```

Related Command(s)

- `ip dhcp pool` - Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- `network` - Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- `show ip dhcp server pools` - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

default-router

Command Objective This command configures the IP address of a default router to which a DHCP client should send packets after booting, for the corresponding DHCP server address pool.

The no form of the command deletes the default router IP address configuration for the DHCP server address pool. The default router IP address configuration is deleted, if the no form of the network command is executed successfully.

Syntax **default-router <ip address>**

no default-router

Mode DHCP Pool Configuration Mode

Notes:

- The configured IP address of the default router should be on the same subnet of the DHCP client.
- The default router IP address configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Example

```
Your product(dhcp-config)# default-router 10.23.2.99
```

Related Command(s)

- ip dhcp pool - Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- network - Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- show ip dhcp server pools - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

option

Command Objective This command configures, for the corresponding DHCP server address pool, the various available DHCP server options with the corresponding specific values. These values can be an ASCII string, hexadecimal string or IP address.

The no form of the command deletes the DHCP server option for the DHCP server address pool. The DHCP server option configuration is deleted, if the no form of the network command is executed successfully.

Syntax **option <code (1-2147483647)> { ascii <string> | hex <Hex String> | ip <address> }**

no option <code (1-2147483647)>

Parameter Description

- `<code (1-2147483647)>` - Configures the unique DHCP option code that represents a specific DHCP option used in a DHCP OFFER message on response to a DHCP DISCOVER message. This value ranges from 1 to 2147483647.
- `ascii<string>` - Configures the ASCII value to be set for the corresponding option code that accepts ASCII string. This value is a character string that should contain only characters from NVT ASCII character set.
- `hex<Hex String>` - Configures the hexadecimal value to be set for the corresponding option code that accepts hexadecimal string.
- `ip<address>` - Configures the unicast IP address to be set for the corresponding option code that accepts IP address.

Mode DHCP Pool Configuration Mode

Default Option code - 1

Note: The DHCP server options configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Example

```
Your product(dhcp-config) # option 19 hex f
```

Related Command(s)

- `ip dhcp pool` - Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- `network` - Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- `show ip dhcp server pools` - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

lease

Command Objective This command configures, for the corresponding DHCP server, the DHCP lease period for an IP address that is assigned from a DHCP server to a DHCP client.

The DHCP lease period represents the time interval (in seconds) till which the DHCP client can use the assigned IP address. The time interval is internally calculated in seconds based on the number of days, hours and minutes configuration.

The no form of the command resets the DHCP lease period to its default value for the DHCP server address pool. The DHCP lease period configuration is deleted and reset, if the no form of the network command is executed successfully.

Syntax **lease { <days (0-365)> [<hours (0-23)> [<minutes (1-59)>]] | infinite }**

no lease

Parameter Description

- `<days (0-365)>` - Configures the number of days that is used to calculate the DHCP lease period. The period also depends on the configured number of hours and minutes. This value ranges from 0 to 365. The value 0 is valid only if either number of hours or minutes is configured with any value other than 0.
- `<hours (0-23)>` - Configures the number of hours that is used to calculate the DHCP lease period. The period also depends on the configured number of days and minutes. This value ranges from 0 to 23. The value 0 is valid only if either number of days or minutes is configured with any value other than 0.
- `<minutes (1-59)>` - Configures the number of minutes that is used to calculate the DHCP lease

period. The period also depends on the configured number of days and hours. This value ranges from 1 to 59.

- `infinite` - Configures the DHCP lease period as 2147483647 seconds.

Mode DHCP Pool Configuration Mode

Default 3600 seconds (1 hour)

Note: The DHCP lease period configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Example

```
Your product(dhcp-config)# lease 1
```

Related Command(s)

- `ip dhcp pool` - Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- `network` - Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- `show ip dhcp server pools` - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

utilization threshold

Command Objective This command configures pool utilization threshold value (in percentage) for the corresponding DHCP server address pool.

The no form of the command resets the pool utilization threshold to its default value for the DHCP server address pool.

If the pool utilization exceeds the configured threshold value, a syslog event and an SNMP trap message are generated. The threshold value ranges from 0 to 100 percentage.

Syntax **utilization threshold { <integer (0-100)> }**

no utilization threshold

Mode DHCP Pool Configuration Mode

Default 75 percent

Note: The pool utilization threshold configuration takes effect only after creating a subnet pool for a DHCP server address pool.

Example

```
Your product(dhcp-config)# utilization threshold 76
```

Related Command(s)

- `ip dhcp pool` - Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- `network` - Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- `show ip dhcp server pools` - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

host hardware-type

Command Objective This command configures host hardware type and its DHCP option with specific values for the corresponding DHCP server address pool.

The no form of the command deletes the hardware type and its DHCP option.

Syntax **host hardware-type <type (1-2147483647)> client-identifier <mac-address> { ip <address> | option <code (1-2147483647)> { ascii <string> | hex <Hex String> | ip <address> }}**

no host hardware-type <host-hardware-type (1-2147483647)> client-identifier <client-mac-address> [{ ip | option <code (1-2147483647)> }]

Parameter Description

- `<type (1-2147483647)>` - Configures the host hardware type for which the host address and the DHCP options needs to be configured. This value ranges from 1 to 2147483647. Only the value 1 is supported, which represents that the hardware type is Ethernet.
- `client identifier<mac-address>` - Configures the DHCP client identifier in a host declaration so that a host record can be found using this client identifier. The client identifier represents the physical address (MAC address) of a network card.
- `ip <address>` - Configures the IPv4 address for the DHCP host.
- option <code (1-2147483647)>- Configures the unique DHCP option code that represents a specific DHCP option used in a DHCP OFFER message on response to a DHCP DISCOVER message. This value ranges from 1 to 2147483647.
  - `ascii<string>` - Configures the ASCII value to be set for the corresponding option code that accepts ASCII string. This value is a character string that should contain only characters from NVT ASCII character set.
  - `hex<Hex String>` - Configures the hexadecimal value to be set for the corresponding option code that accepts hexadecimal string.
  - `ip <address>` - Configures the unicast IP address to be set for the corresponding option code that accepts IP address.

Mode DHCP Pool Configuration Mode

Example

```
Your product(dhcp-config)# host hardware-type 1 client- identifier
00:11:22:33:44:55 option 1 ip 10.0.0.1
```

Related Command(s)

- `ip dhcp pool` - Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- `show ip dhcp server pools` - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.
- `show ip dhcp server binding` - Displays the DHCP server binding information

debug ip dhcp server

Command Objective This command enables the tracking of the DHCP server operations as per the configured debug levels. The debug statements are generated for the configured trace levels.

The no form of the command disables the tracking of the DHCP server operations. The debug statements are not generated for the configured trace levels.

This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

Syntax **debug ip dhcp server { all | events | packets | errors | bind | linkage }**

no debug ip dhcp server { all | events | packets | errors | bind | linkage}

Parameter Description

- `all` - Generates debug statements for all kind of failure traces.
- `events` - Generates debug statements for DHCP server events that provide DHCP server service status. The DHCP server events are generated when any of packets are sent successfully or when an ACK is received.
- `packets` - Generates debug statements for packet related messages. These messages are generated for all events generated during processing of packets.
- `errors` - Generates debug statements for trace error code debug messages. These messages are generated for all error events generated.
- `bind` - Generates debug statements for trace bind messages. These messages are generated when a DHCP ACK is received.
- `linkage` - Generates debug statements for database linkage messages. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode Privileged EXEC Mode

Default Tracking of the DHCP server operations is disabled

Example

```
Your product# debug ip dhcp server all
```

Related Command(s)

- `show ip dhcp server information` - Displays the DHCP server configuration information.
- `show debugging` - Displays state of each debugging option

show ip dhcp server information

Command Objective This command displays the DHCP server configuration information.

The information contains status of DHCP server, ICMP echo mechanism status, debug level, boot server IP address, boot file name and server offer reuse time.

Syntax **show ip dhcp server information**

Mode Privileged EXEC Mode

Example

```
Your product# show ip dhcp server information
DHCP server status                 : Enable
Send Ping Packets                  : Disable
Debug level                        : None
Server Address Reuse Timeout       : 5 secs
Next Server Adress                 : 0.0.0.0
Boot file name                     : None
```

Related Command(s)

- `service dhcp-server` - Enables the DHCP server in the switch (that is, switch acts as DHCP server).
- `ip dhcp next-server` - Sets the IP address of the boot server (that is, TFTP server) from which the initial boot file is to be loaded.
- `ip dhcp bootfile` - Configures the name of the initial boot file to be loaded in a DHCP client.
- `ip dhcp` - Enables ICMP echo mechanism or configures offer-reuse timeout for the DHCP server.
- `debug ip dhcp server` - Enables the tracking of the DHCP server operations as per the configured debug levels.

show ip dhcp server pools

Command Objective This command displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

Syntax **show ip dhcp server pools**

Mode Privileged EXEC Mode

Example

```
Your product# show ip dhcp server pools
```

```
  Global Options

----------------------------
 Code      :   19, Value     : 0
 Pool Id                       : 1
------------------------------------------------------------------------------------
 Subnet Mask                   : 255.0.0.0
 Lease time                    : 86400 secs
 Utilization threshold         : 76%
 Start Ip                      : 20.0.0.1
 End Ip                        : 20.0.0.50
 Exclude Address Start IP      : 20.0.0.1
 Exclude Address End IP        : 20.0.0.30
 Subnet Options
----------------------------
 Code      :    1, Value     : 255.0.0.0
 Code      :    3, Value     : 10.23.2.99
 Code      :    6, Value     : 20.0.0.1
 Code       :   15, Value     : SMIS
 Code      :   19, Value     : 0
Code       :    44, Value      : 20.0.0.3
 Code       :    46, Value      : 8
 Host Options
 -------------------
 Hardware type                    : 1
 Client Identifier                : 00:11:22:33:44:55
 Code       :     1, Value      : 10.0.0.1
```

Related Command(s)

- `ip dhcp option` - Configures globally the various available DHCP server options with the corresponding specific values
- `ip dhcp pool` - Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- `network` - Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.
- `excluded-address` - Creates an excluded pool that defines a range of IP addresses which needs to be excluded from the created subnet pool.
- `domain-name` - Configures the domain name option for the corresponding DHCP server address pool.
- `dns-server` - Configures the IP address of a DNS server for the corresponding DHCP server address pool.
- `netbios-name-server` - Configures the IP address of a NetBIOS and WINS name server that is available to Microsoft DHCP clients.
- `netbios-node-type` - Configures the NetBIOS node type for Microsoft DHCP clients, for the corresponding DHCP server address pool.
- `default-router` - Configures the IP address of a default router to which a DHCP client should send packets after booting, for the corresponding DHCP server address pool.
- `option` - Configures, for the corresponding DHCP server address pool, the various available DHCP server options with the corresponding specific values.
- `lease` - Configures, for the corresponding DHCP server, the DHCP lease period for an IP address that is assigned from a DHCP server to a DHCP client.
- `utilization threshold` - Configures pool utilization threshold value (in percentage) for the corresponding DHCP server address pool.
- `host hardware-type` - Configures host hardware type and its DHCP option with specific values for the corresponding DHCP server address pool.
- `show ip dhcp server statistics` - Displays various DHCP server statistics related information such as number of DHCPDECLINE messages received, DHCPOFFER messages sent and so on.

show ip dhcp server binding

Command Objective This command displays the DHCP server binding information.

A DHCP binding is created when a DHCP server assigns an IP address to a DHCP client. The information contains the allocated IP address, host hardware type, host hardware address, binding state and expiry time of the allocated DHCP lease.

Syntax **show ip dhcp server binding**

Mode Privileged EXEC Mode

Note: The DHCP server binding information is displayed, only if the DHCP server is enabled and the DHCP binding is created.

Example

```
Your product# show ip dhcp server binding
Ip                       Hw Hw     Binding       Expire
Address                  Type      Address       State  Time
------------             -------   ------------  ---------- ----------
12.0.0.2
13:22:41                 Ethernet
2009                     00:02:02:03:    4:01 Assigned May 12
```

Related Command(s)

- `service dhcp-server` - Enables the DHCP server in the switch.
- `ip dhcp` - Enables ICMP echo mechanism or configures offer-reuse timeout for the DHCP server.
- `host hardware-type` - Configures host hardware type and its DHCP option with specific values for the corresponding DHCP server address pool.

show ip dhcp server statistics

Command Objective This command displays various DHCP server statistics related information such as number of DHCPDECLINE messages received, DHCPOFFER messages sent and so on.

Syntax **show ip dhcp server statistics**

Mode Privileged EXEC Mode

Example

```
Your product# show ip dhcp server statistics
Address pools :
Message                  2
Received
-------------------------------------------    ---------------
DHCPDISCOVER               6
DHCPREQUEST                2
DHCPDECLINE                0
DHCPRELEASE                0
DHCPINFORM                 0
Message                    Sent
-------                    ----
DHCPOFFER                  6
DHCPACK                    2
DHCPNAK                    0
```

Related Command(s)

- `service dhcp-server` - Enables the DHCP server in the switch.
- `ip dhcp pool` - Creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized.
- `ip dhcp` - Enables ICMP echo mechanism or configures offer-reuse timeout for the DHCP server.
- `show ip dhcp server pools` - Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.

24 IGMP Snooping

Internet Group Multicast Protocol, (IGMP) is the protocol, a host uses to inform a router when it joins (or leaves) an Internet multicast group. IGMP is only used on a local network; a router must use another multicast routing protocol to inform other routers of group membership. IGMP Snooping (IGS) is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers. In IGS, a host computer uses IGMP to inform a router that it intends to listen to a specific multicast address. If another computer snoops such packets, it can learn the multicast sessions to which other computers on the local network are listening. The multicast packet transfer happens only between the source and the destination computers. Broadcasting of packets is avoided. IGMP snooping significantly reduces traffic from streaming media and other bandwidth-intensive IP multicast applications.

The list of CLI commands for the configuration of IGS is common to both Single Instance and Multiple Instance except for a difference in the prompt that appears for the Switch with Multiple Instance support.

The prompt for the Global Configuration Mode is,

Your Product(config)#

The list of CLI commands for the configuration of IGS is as follows:

- ip igmp snooping
- ip igmp snooping proxy-reporting
- snooping multicast-forwarding-mode
- ip igmp snooping mrouter-time-out
- ip igmp querier-timeout
- ip igmp snooping port-purge-interval
- ip igmp snooping source-only learning age-timer
- ip igmp snooping report-suppression interval
- ip igmp snooping retry-count
- ip igmp snooping group-query-interval
- ip igmp snooping report-forward

- ip igmp snooping query-forward
- ip igmp snooping version
- ip igmp snooping fast-leave
- ip igmp snooping vlan - immediate leave
- ip igmp snooping querier
- ip igmp snooping query-interval
- ip igmp snooping startup-query-interval
- ip igmp snooping other-querier-present-interval
- ip igmp snooping mrouter
- ip igmp snooping vlan mrouter
- shutdown snooping
- debug ip igmp snooping
- snooping leave-process config-level
- ip igmp snooping enhanced-mode
- ip igmp snooping sparse-mode
- snooping report-process config-level
- ip igmp snooping multicast-vlan
- mvr
- ip igmp snooping filter
- ip igmp snooping blocked-router
- ip igmp snooping multicast-vlan profile
- ip igmp snooping leavemode
- ip igmp snooping ratelimit
- ip igmp snooping limit
- ip igmp snooping filter-profileId
- ip igmp snooping proxy
- ip igmp snooping max-response-code
- ip igmp snooping mrouter-port –time-out
- ip igmp snooping mrouter-port-version
- show ip igmp snooping mrouter
- show ip igmp snooping mrouter - Redundancy
- show ip igmp snooping globals
- show ip igmp snooping
- show ip igmp snooping - Redundancy
- show ip igmp snooping groups
- show ip igmp snooping forwarding-database
- show ip igmp snooping forwarding-database - Redundancy
- show ip igmp snooping statistics
- show ip igmp snooping blocked-router
- show ip igmp snooping multicast-receivers
- show ip igmp snooping port-cfg
- show ip igmp snooping multicast-vlan
- ip igmp snooping clear counters

- ip igmp snooping send-query
- ip igmp snooping static-group

ip igmp snooping

Command Objective	This command enables IGMP snooping in the switch/ a specific VLAN. When snooping is enabled in a switch or interface, it learns the hosts intention to listen to a specific multicast address. When the switch receives any packet from the specified multicast address, it forwards the packet to the host listening for that address. Broadcasting is avoided to save bandwidth. When IGMP snooping is enabled globally, it is enabled in all the existing VLAN interfaces.

The no form of the command disables IGMP snooping in the switch/a specific VLAN. When IGMP snooping is disabled globally, it is disabled in all the existing VLAN interfaces.

Syntax	**Global Configuration Mode**

ip igmp snooping [vlan <vlanid/vfi_id>]

no ip igmp snooping [vlan <vlanid/vfi_id>]

Config-VLAN Mode

ip igmp snooping

no ip igmp snooping

Parameter Description

- `vlan <vlan-id/vfi-id>` - Enables IGMP snooping for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
    - `<vlan -id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094.
    - `<vfi-id>.` - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.
        - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
        - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
        - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

Mode	Global Configuration Mode / Config-VLAN Mode

Default IGMP snooping is globally disabled, and in all VLANs.

Note: GMRP has to be disabled for enabling the IGMP snooping.

Example

```
Your Product(config)# ip igmp snooping
Your Product(config-vlan)# ip igmp snooping
```

Related Command(s)

- `shutdown snooping` - Shuts down IGMP snooping in the switch.
- `ip igmp snooping fast-leave / ip igmp snooping vlan - immediate leave` - Enables fast leave processing and IGMP snooping for a specific VLAN
- `show ip igmp snooping` - Displays IGMP snooping information for all VLANs or a specific VLAN.
- `show ip igmp snooping globals` - Displays the IGMP snooping information for all VLANs or a specific VLAN.
- `snooping multicast-forwarding-mode` – Specifies the snooping multicast forwarding mode.
- `show ip igmp snooping multicast-receivers` – Displays IGMP multicast host information for all VLANs or a specific VLAN or specific VLAN and group address for a given switch or for all switches (if no switch is specified).
- `show ip igmp forwarding-database` - Displays multicast forwarding entries

ip igmp snooping proxy-reporting

Command Objective This command enables proxy reporting in the IGMP snooping switch. When enabled, the switch supports the multicast router to learn the membership information of the multicast group. It forwards the multicast packets based on group membership information. The proxy-reporting switch acts as a querier to the downstream hosts. It sends proxy-reporting to upstream queriers.

The no form of the command disables proxy reporting in the IGMP snooping switch.

Syntax **ip igmp snooping proxy-reporting**

no ip igmp snooping proxy-reporting

Mode Global Configuration Mode

Default Proxy-reporting is enabled

Note: Proxy reporting can be enabled in the IGMP snooping switch only if the proxy is disabled in the switch.

Example

```
Your Product(config)# ip igmp snooping proxy-reporting
```

Related Command(s)

- no ip igmp snooping proxy – Disables proxy in the IGMP snooping switch.

- show ip igmp snooping globals - Displays the IGMP snooping information for all VLANs or a specific VLAN

- show ip igmp forwarding-database - Displays multicast forwarding entries

snooping multicast-forwarding-mode

Command Objective This command specifies the snooping multicast forwarding mode (IP based or MAC based). When ip mode is selected, and PIM and IGS are enabled, the L3 bitmap in the IPMC table is updated by PIM. The corresponding L2 bitmap is updated by querying the IGS to obtain Portlist. When PIM is disabled, IGS updates the L2 bitmap in the IPMC table directly. When the mode is MAC based, the L2 bitmap is updated by PIM which queries the VLAN to obtain Portlist. When PIM is disabled, the IGS updates the L2 bitmap directly.

Syntax **snooping multicast-forwarding-mode {ip | mac}**

Parameter Description

- `ip` - Configures the multicast forwarding mode as IP Address based. The PIM queries the IGS module to obtain the Portlist.
- `mac` - Configures the multicast forwarding mode as MAC Address based. The PIM queries the VLAN to obtain the Portlist.

Mode Global Configuration Mode

Default mac

Example

```
Your Product(config)# snooping multicast-forwarding-mode mac
```

Related Command(s)

- `show ip igmp snooping globals` - Displays the IGMP snooping information for all VLANs or a specific VLAN
- `ip igmp snooping enhanced-mode` - Enables/disables snooping system enhanced mode in the switch.
- `ip igmp snooping static-group` - Configure IGMP snooping static multicast for Vlan(s)

ip igmp snooping mrouter-time-out

Command Objective This command sets the IGMP snooping router port purge time-out interval.

Snooping learns the available router ports and initiates router port purge time- out timer for each learnt router port. The router sends control messages to the ports. If the router ports receive such control messages, the timer is restarted. If no message is received by the router ports before the timer expires, the router port entry is purged. The purge time-out value ranges between 60 and 600 seconds.

The no form of the command sets the IGMP snooping router port purge time- out to default value.

Syntax **ip igmp snooping mrouter-time-out <(60 – 600) seconds>**

no ip igmp snooping mrouter-time-out

Mode Global Configuration Mode

Default 125 seconds

Example Your Product(config)#ip igmp snooping mrouter-time-out 70

Related Command(s)

- `show ip igmp snooping mrouter` - Displays detailed information about the router ports for all VLANs or specific VLAN
- `show ip igmp snooping globals` - Displays the global information of IGMP snooping

ip igmp querier-timeout

Command Objective This command sets the IGMP snooping router port purge time-out interval. Snooping learns the available router ports and initiates router port purge time- out timer for each learnt router port. The routers send control messages to the ports. If the router ports receive such control messages, the timer is restarted. If no message is received by the router ports before the timer expires, the router port entry is purged. The purge time-out value ranges between 60 and 600 seconds.

This command is a standardized implementation of the existing command; ip igmp snooping mrouter-time-out. It operates similar to the existing command.

Syntax **ip igmp querier-timeout <(60 - 600) seconds>**

Mode Global Configuration Mode

Default 125 seconds

Example `Your Product(config)#ip igmp querier-timeout 70`

Related Command(s)

- `show ip igmp snooping mrouter` - Displays detailed information about the router ports for all VLANs or specific VLAN
- `show ip igmp snooping globals` - Displays the global information of IGMP snooping

ip igmp snooping port-purge-interval

Command Objective This command configures the IGMP snooping port purge time interval. When the port receives reports from hosts, the timer is initiated. If the port receives another report before the timer expires, the timer is restarted. If the port does not receive any report from hosts till the timer expires, then the port entry is purged from the multicast database. The purge time interval value ranges between 130 and 1225 seconds.

The no form of the command sets the IGMP snooping port purge time to default value.

Syntax **ip igmp snooping port-purge-interval <(130 - 1225) seconds>**

no ip igmp snooping port-purge-interval

Mode Global Configuration Mode

Default 260 seconds

Example

```
Your Product (config)# ip igmp snooping port-purge- interval 150
```

Related Command(s)

- `show ip igmp snooping`- Displays IGMP snooping information for all VLANs or a specific VLAN.
- `show ip igmp snooping globals` - Displays the IGMP snooping information for all VLANs or a specific VLAN

ip igmp snooping source-only learning age-timer

Command Objective This command configures the IGMP snooping port purge time interval. When the port receives reports from hosts, the timer is initiated. If the port receives another report before the timer expires, the timer is restarted. If the port does not receive any report from hosts till the timer expires, then the port entry is purged from the multicast database. The purge time interval value ranges between 130 and 1225 seconds.

This command is a standardized implementation of the existing command; ip igmp snooping port-purge-interval. It operates similar to the existing command.

Syntax **ip igmp snooping source-only learning age-timer <short(130-1225)>**

no ip igmp snooping source-only learning age-timer

Mode Global Configuration Mode

Default 260 seconds

Example

```
Your Product (config)# ip igmp snooping source-only learning age-timer 200
```

Related Command(s)

- `show ip igmp snooping`- Displays IGMP snooping information for all VLANs or a specific VLAN.
- `show ip igmp snooping globals` - Displays the IGMP snooping information for all VLANs or a specific VLAN

ip igmp snooping report-suppression interval

Command Objective This command sets the IGMP snooping report-suppression time interval. The switch forwards IGMPv2 report message to the multicast group. A timer is started immediately after forwarding the report message and runs for set period of time. During this interval the switch does not forward another IGMPv2 report message addressed to the same multicast group to the router ports.

The no form of the command sets the IGMP snooping report-suppression interval time to the default value.

Syntax **ip igmp snooping report-suppression-interval <(1 – 25) seconds>**

no ip igmp snooping report-suppression-interval

Mode Global Configuration Mode

Default 5 seconds

Note: The ip igmp snooping report-suppression-interval is used only when the proxy and proxy-reporting are disabled.

Example

```
Your Product(config)# ip igmp snooping report-suppression- interval 20
```

Related Command(s) `show ip igmp snooping globals` - Displays the IGMP snooping information for all VLANs or a specific VLAN

ip igmp snooping retry-count

Command Objective This command sets the maximum number of group specific queries sent by the switch to check if there are any interested v2 receivers for the group when it receives a leave message in the proxy/ proxy-reporting mode. The port is deleted from the group membership information in the forwarding database if the maximum retry count exceeds set number. This value ranges between 1 and 5.

The no form of the command sets the number of group specific queries sent by the switch on reception of leave message to default value.

Syntax **ip igmp snooping retry-count <1 - 5>**

no ip igmp snooping retry-count

Mode Global Configuration Mode

Default 2

Example

```
Your Product (config)# ip igmp snooping retry-count 4
```

Related Command(s)

- `show ip igmp snooping globals` - Displays the IGMP snooping information for all VLANs or a

specific VLAN
- `ip igmp snooping clear counters` - Clears the IGMP snooping statistics maintained for Vlan(s).

ip igmp snooping group-query-interval

Command Objective This command sets the time interval after which the switch sends a group specific query to find out if there are any interested receivers in the group when it receives a leave message. If it does not receive a response from the group, the port is removed from the group membership information in the forwarding database. This value ranges between 2 and 5.

The no form of the commands sets the group specific query interval time to default value.

Syntax **ip igmp snooping group-query-interval <2-5) seconds>**

no ip igmp snooping group-query-interval

Mode Global Configuration Mode

Default 2 seconds

Example `Your Product(config)# ip igmp snooping group-query-interval 3`

Related Command(s)

- `show ip igmp snooping globals` - Displays the IGMP snooping information for all VLANs or a specific VLAN
- `show ip igmp snooping statistics` - Displays IGMP snooping statistics for all VLANs or a specific VLAN
- `show ip igmp snooping groups` - Displays IGMP group information for all VLANs or a specific VLAN

ip igmp snooping report-forward

Command Objective This command configures the IGMP reports to be forwarded to all ports, router ports of a VLAN or non-edge ports. The configuration enables the switch to forward IGMP report messages to the selected ports thus avoiding flooding of the network.

The no form of the command sets IGMP report-forwarding status to default value.

Syntax **ip igmp snooping report-forward {all-ports | router-ports | non-edge-ports }**

no ip igmp snooping report-forward

Parameter Description

- `all-ports` - Configures the IGMP reports to be forwarded to all the ports of a VLAN
- `router-ports` - Configures the IGMP reports to be forwarded only to router ports of a VLAN

- `non-edge-ports` - Configures the IGMP reports to be forwarded only to STP non edge ports

Mode Global Configuration Mode

Default router-ports

Note: In snooping mode, snooping module will forward reports only on router ports by default.

Example

```
Your Product(config)# ip igmp snooping report-forward all- ports
```

Related Command(s) `show ip igmp snooping globals` - Displays the IGMP snooping information for all VLANs or a specific VLAN

ip igmp snooping query-forward

Command Objective This command configures the IGMP queries to be forwarded to all Vlan member ports or only to non-router ports. This configuration directs the queries to the selected ports to avoid flooding of the network. The queries are forwarded to multicast groups. If the Vlan module is enabled, IGMP snooping sends and receives the multicast packets through Vlan module. When Vlan is disabled, it sends the multicast packets through Bridge initialization/shutdown sub module.

Syntax **ip igmp snooping query-forward {all-ports | non-router- ports}**

Parameter Description

- `all-ports` - Configures the IGMP query forward administrative control status as all VLAN member ports. This is done to find out if there are any interested listeners in the network.
- `non-router-ports` - Configures the IGMP query forward administrative control status as non-router ports only. This is done to reduce the traffic in the network.

Mode Global Configuration Mode

Default non-router-ports

Example

```
Your Product(config)# ip igmp snooping query-forward all- ports
```

Related Command(s) `show ip igmp snooping globals` - Displays the IGMP snooping information for all VLANs or a specific VLAN.

ip igmp snooping version

Command Objective This command configures the operating version of the IGMP snooping switch for a specific VLAN. The version can be set manually to execute condition specific commands.

Syntax **ip igmp snooping version { v1 |v2 | v3}**

Parameter Description

- v1 - Configures the version as IGMP snooping Version 1.
- v2 - Configures the version IGMP snooping Version 2.
- v3 - Configures the version IGMP snooping Version 3.

Mode Config-VLAN Mode

Default v3

Example

```
Your Product(config-vlan)#ip igmp snooping version v2
```

Related Command(s)

- `show ip igmp snooping` - Displays IGMP snooping information for all VLANs or a specific VLAN.
- `show ip igmp forwarding-database` - Displays multicast forwarding entries.

ip igmp snooping fast-leave

Command Objective This command enables fast leave processing and IGMP snooping for a specific VLAN. It enables IGMP snooping only for the specific VLAN, when IGMP snooping is globally disabled. When the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received.

The no form of the command disables fast leave processing for a specific VLAN.

Syntax **ip igmp snooping fast-leave**

no ip igmp snooping fast-leave

Mode Config-VLAN Mode

Default Fast leave processing is disabled

Note: Fast leave configurations done in a VLAN when IGMP snooping is disabled in a VLAN, will be applied only when IGMP snooping is enabled in the VLAN.

Example

```
Your Product (config-vlan)# ip igmp snooping fast-leave
```

Related Command(s)

- `ip igmp snooping` - Enables IGMP snooping in the switch/a specific VLAN
- `show ip igmp snooping` - Displays IGMP snooping information for all VLANs or a specific VLAN
- `show ip igmp snooping globals` - Displays the global information of IGMP snooping

ip igmp snooping vlan - immediate leave

Command Objective This command enables fast leave processing and IGMP snooping for a specific VLAN, It enables IGMP snooping only for the specific VLAN, when IGMP snooping is globally disabled.

When the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received. The ID of the VLAN ranges between 1 and 4094.

The no form of the command disables fast leave processing for a specific VLAN.

This command is a standardized implementation of the existing command; ip igmp snooping fast-leave. It operates similar to the existing command.

Syntax **ip igmp snooping vlan <vlanid(1-4094)> immediate-leave**

no ip igmp snooping vlan <vlanid(1-4094)> immediate-leave

Mode Global Configuration Mode

Default Fast leave processing is disabled in all the VLANs

Note: Fast leave configurations done in a VLAN when IGMP snooping is disabled in a VLAN, will be applied only when IGMP snooping is enabled in the VLAN.

Example

```
Your Product (config)# ip igmp snooping vlan 1 immediate- leave
```

Related Command(s)

- `ip igmp snooping` - Enables IGMP snooping in the switch/a specific VLAN
- `show ip igmp snooping` - Displays IGMP snooping information for all VLANs or a specific VLAN.

ip igmp snooping querier

Command Objective This command configures the IGMP snooping switch as a querier for a specific VLAN. When configured as a querier, the switch sends IGMP query messages. The query messages will be suppressed if there are any routers in the network.

The no form of the command configures the IGMP snooping switch as non- querier for a specific VLAN.

Syntax **ip igmp snooping querier**

no ip igmp snooping querier

Mode Config-VLAN Mode

Default Non-querier

Example

```
Your Product (config-vlan)# ip igmp snooping querier
```

Related Command(s) `show ip igmp snooping` - Displays IGMP snooping information for all VLANs or a specific VLAN

ip igmp snooping query-interval

Command Objective This command sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN. The switch sends querier messages in proxy mode and proxy-reporting mode to all downstream interfaces for this time interval. The value range is between 60 to 600 seconds.

The no form of the command sets the IGMP querier interval to default value.

Syntax **ip igmp snooping query-interval <(60 - 600) seconds>**

no ip igmp snooping query-interval

Mode Config-VLAN Mode

Default 125 Seconds

Notes:

- The switch must be configured as a querier for this configuration to be imposed.
- In proxy reporting mode, general queries are sent on all downstream interfaces with this interval only if the switch is the Querier.
- In proxy mode, general queries will be sent on all downstream interfaces with this interval.

Example

```
Your Product (config-vlan) # ip igmp snooping query- interval 200
```

Related Command(s) `show ip igmp snooping` - Displays IGMP snooping information for all VLANs or a specific VLAN

ip igmp snooping startup-query-interval

Command Objective This command sets the time interval between the general query messages sent by the IGMP snooping switch, during startup of the querier election process. This time interval ranges between 15 and 150 seconds and should be less than or equal to query interval/ 4.

The no form of the command sets the IGMP startup query interval to the default value.

Syntax **ip igmp snooping startup-query-interval <(15 - 150) seconds>**

no ip igmp snooping startup-query-interval

Mode Config-VLAN Mode

Default 31 Seconds

Notes:

- The switch should be configured as querier for the startup query interval command to produce results.
- The startup query interval should be less than or equal to ¼ of the query interval.

Example `Your Product(config-vlan) # ip igmp snooping startup-query- interval 100`

Related Command(s)

- `ip igmp snooping query-interval` - Sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN
- `show ip igmp snooping querier` - Displays IGMP snooping information for all VLANs or a specific VLAN
- `show ip igmp snooping` - Displays IGMP snooping information for all VLANs or a specific VLAN for a given context or for all the contexts.

ip igmp snooping startup-query-count

Command Objective This command sets the maximum number of general query messages sent out on switch startup, when the switch is configured as a querier. This value ranges between two and five. Startup query messages are sent to announce the presence of the switch along with its identity. The startup query count is manually configured to change the existing count. This value ranges between 2 and 5.

The no form of the command sets the number of general query messages sent out on switch startup, when the switch is configured as a querier to default value.

Syntax **ip igmp snooping startup-query-count <2 - 5>**

no ip igmp snooping startup-query-count

Mode Config-VLAN Mode

Default 2

Note: The switch should be configured as a querier for startup query count configuration to be effective.

Example `Your Product (config-vlan) # ip igmp snooping startup- query-count 4`

Related Command(s)

- `ip igmp snooping querier` - Configures the IGMP snooping switch as a querier for a specific VLAN
- `ip igmp snooping query-interval` - Sets the time period with which the general queries are sent by the IGMP snooping switch
- `ip igmp snooping clear counters` - Clears the IGMP snooping statistics maintained for Vlan(s).
- `show ip igmp snooping` - Displays IGMP snooping information for all VLANs or a specific VLAN

ip igmp snooping other-querier-present-interval

Command Objective This command sets the maximum time interval to decide that another querier is present in the network. This time interval ranges between 120 and 1215 seconds. Within this time interval if the querier receives response from another querier, then the one with a higher IP address is announced as the querier for the network. The other querier present interval must be greater than or equal to ((Robustness Variable * Query Interval) + (Query Response Interval/2)). Here, Robustness value is 2.

The no form of the command resets this interval to default value.

Syntax **ip igmp snooping other-querier-present-interval <value(120-1215) seconds>**

no ip igmp snooping other-querier-present-interval

Mode Config-VLAN Mode

Default 255 Seconds

Note: The switch should be configured as a querier for the other querier present command to be effective.

Example

```
Your Product(config-vlan) # ip igmp snooping other-querier- present-
interval 200
```

Related Command(s)

- `ip igmp snooping querier` - Configures the IGMP snooping switch as a querier for a specific VLAN
- `ip igmp snooping query-interval` - Sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN.
- `ip igmp snooping max-response-code` - Sets the maximum response code inserted in general queries send to host.
- `show ip igmp snooping`- Displays IGMP snooping information for all VLANs or a specific VLAN.

ip igmp snooping mrouter

Command Objective This command enables IGMP snooping and configures a list of multicast router ports for a specific VLAN, when IGMP snooping is globally enabled. This will enable IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled.

Any IGMP message received on a switch is forwarded only on the router-ports and not on the host ports. In this manner, the IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network.

The no form of the command deletes the statically configured router ports for a VLAN.

Syntax **ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...>**

no ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...>

Parameter Description

- `<interface-type>` - Configures list of multicast router ports for the specified type of interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<0/a-b, 0/c, ...>` - Sets list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID isprovided, for interface type port-channel. Use comma asa separator without space while configuring list of interfaces. Example: 0/1,0/3 or 1, 3.

Mode Config-VLAN Mode

Note: The list of multicast router ports configured while IGMP snooping is disabled in the VLAN is applied only when the IGMP snooping is enabled in the VLAN.

Example

```
Your Product (config-vlan)# ip igmp snooping mrouter gigabitethernet 0/1-3
```

Related Command(s)

- `ip igmp snooping` - Enables IGMP snooping in the switch/a specific VLAN
- `show ip igmp snooping mrouter` - Displays the router ports for all VLANs or specific VLAN.
- `ip igmp snooping mrouter-port` –time-out - Configures the router port purge time-out interval for a VLAN.
- `ip igmp snooping mrouter-port-version` - Configures the operating version of the router port for a VLAN.

ip igmp snooping vlan mrouter

Command Objective This command enables IGMP snooping and configures a list of multicast router ports for a specific VLAN, if IGMP snooping is globally enabled. This will enable IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled.

Any IGMP message received on a switch is forwarded only on the router-ports and not on host ports. In this manner, the IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network.

The no form of the command deletes the statically configured router ports for a VLAN.
This command is a standardized implementation of the existing command; ip igmp snooping mrouter. It

operates similar to the existing command.

Syntax **ip igmp snooping vlan <vlanid (1-4094)> mrouter <ifXtype> <0/a-b, 0/c, ...>**

no ip igmp snooping vlan <vlanid (1-4094)> mrouter <ifXtype> <0/a-b, 0/c, ...>

Parameter Description

- `<vlanid (1-4094)>` - Configures the VLAN for which the list of multicast router ports should be configured statically. This is a unique value that represents the specific L3 VLAN created. An L3 VLAN interface is a VLAN that is mapped to an IP interface and assigned an IP address. This value ranges between 1 and 4094.
- `<ifXtype>` - Configures the list of multicast router ports for the specified type of interface. The interface can be:
    - `qx-ethernet` **–**A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` **–** A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
    - `extreme-ethernet` **–** A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - `port-channel` **–** Logical interface that represents an aggregator which contains several ports aggregated together.
- `<0/a-b, 0/c, ...>` - Sets the list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3.

Mode Global Configuration Mode

Note: The list of multicast router ports configured while IGMP snooping is disabled in the VLAN is applied only when the IGMP snooping is enabled in the VLAN.

Example

```
Your Product(config)# ip igmp snooping vlan 1 mrouter gigabitethernet 0/1
```

Related Command(s)

- `ip igmp snooping` - Enables IGMP snooping in the switch/a specific VLAN
- `show ip igmp snooping mrouter` - Displays the router ports for all VLANs or specific VLAN
- `ip igmp snooping mrouter-port -time-out` - Configures the router port purge time-out interval for a VLAN
- `ip igmp snooping mrouter-port-version` - Configures the operating version of the router port for a VLAN

shutdown snooping

Command Objective This command shuts down snooping in the switch. When the user does not require the IGMP snooping module to be running, it can be shut down. When shut down, all resources acquired by the Snooping Module are released to the system. For the IGS feature to be functional on the switch, the 'system-control' status must be set as 'start' and the 'state' must be 'enabled'.

The no form of the command starts and enables snooping in the switch.

Syntax **shutdown snooping**

no shutdown snooping

Mode Global Configuration Mode

Default Snooping is enabled

Note: Snooping cannot be started in the switch, if the base bridge mode is configured as transparent bridging.

Example

```
Your Product(config)# shutdown snooping
```

Related Command(s)

- base bridge-mode - Configures the mode in which the VLAN feature should operate on the switch.
- ip igmp snooping - Enables IGMP snooping in the switch/a specific VLAN

debug ip igmp snooping

Command Objective This command configures the various debug and trace statements to handle error and event management available in the igmp snooping module. The traces are enabled by passing the necessary parameters.

The no form of the command resets debug options for IGMP snooping module.

Syntax **debug ip igmp snooping {[init][resources][tmr][src][grp][qry] [vlan][pkt][fwd][mgmt][redundancy] | all } [switch <switch_name>]**

no debug ip igmp snooping {[init][resources][tmr][src][grp][qry] [vlan][pkt][fwd][mgmt][redundancy] | all } [switch <switch_name>]

Parameter Description

- `init` - Generates Init and Shutdown trace messages at the instances when the module is initiated or shutdown. The information is logged in a file.
- `resources` - Generates System Resources management trace messages when there is a change in the resource status. The information is logged in a file.

- `tmr` - Generates Timer trace messages at the instances where timers are involved. The information is logged ina file.
- `src` - Generates trace messages when Source Information is involved.
- `grp` - Generates trace messages when Group Information is involved.
- `qry` - Generates trace messages when Query messages are sent or received.
- `vlan` - Generates trace messages when VLAN related Information is involved.
- `pkt` - Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets.
- `fwd` - Generates traces messages when forwarding Database is involved.
- `mgmt` - Generates debug statements for management plane functionality traces.
- `redundancy` - Generates debug statements for redundancy code flow traces. This trace is generated when there is a failure in redundancy processing.
- `all` - Generates all types of trace messages
- `switch <switch_name>` - Generates switch related trace messages.

Mode Privileged EXEC Mode

Default Debugging is Disabled.

Example

```
Your Product# debug ip igmp snooping fwd
```

Related Command(s) `show debugging` - Displays state of each debugging option

snooping leave-process config-level

Command Objective This command specifies the level of configuring the leave processing mechanisms. When the switch intercepts a leave group message on a switch port, it normally sends a query to that multicast group through the same switch port. If no hosts respond to the query and no multicast routers have been discovered on the switch port, that port is removed from the multicast group.

Syntax **snooping leave-process config-level {vlan | port}**

Parameter Description

- `vlan` - Configures the leave mechanism at the Vlan level. In Vlan based leave processing mode, the fast leave functionality configurable per vlan or normal leave configurations are available for processing leave messages.
- `port` - Configures the leave mechanism at port level. In Port based leave processing mode, the explicit host tracking functionality, the fast leave functionality or normal leave configurable on a interface are used for processing the leave messages.

Mode Global Configuration Mode

Default vlan

Example

```
Your Product(config)# snooping leave-process config-level port
```

Related Command(s)

- `ip igmp snooping leavemode` – Configures the port leave mode for an interface.
- `show ip igmp snooping globals` – Displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switch (if switch is not specified)

ip igmp snooping enhanced-mode

Command Objective This command configures snooping system enhanced mode in the switch. It is a mode of operation provided to enhance the operation of IGMP snooping module to duplicate Multicast traffic by learning Multicast group entries based on the Port and Inner Vlan. This mode of operation is applied when the down stream devices are less intelligent or not capable of duplicating Multicast traffic.

Syntax **ip igmp snooping enhanced-mode { enable | disable }**

Parameter Description

- `enable` - Enables snooping system enhanced mode in the switch.
- `disable` - Disables snooping system enhanced mode in the switch.

Mode Global Configuration Mode

Default disable

Note: Enhanced mode is in enabled state only when the snooping mode is set as IP Based

Example

```
Your Product(config)# ip igmp snooping enhanced-mode enable
```

Related Command(s)

- `snooping multicast-forwarding-mode` – Specifies the snooping multicast forwarding mode.
- `show ip igmp snooping globals` – Displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switch (if switch is not specified).
- `ip igmp snooping leavemode` – Configures the port leave mode for an interface.
- `ip igmp snooping ratelimit` – Configures the rate limit for a downstream interface in units of the number of IGMP packets per second.
- `ip igmp snooping limit` – Configures the maximum limit type for an interface.
- `ip igmp snooping filter-profileId` – Configures the multicast profile index for a downstream interface.

ip igmp snooping sparse-mode

Command Objective This command configures snooping system sparse mode in the switch. In the sparse mode, the IGS module drops the unknown multicast traffic when there is no listener for the multicast data. In the non-sparse-mode, the IGS module forwards the unknown multicast traffic. The multicast data gets flooded to the member port of vlan.

Syntax **ip igmp snooping sparse-mode { enable | disable }**

Parameter Description

- enable - Enables snooping system sparse mode in the switch. Drops unknown multicast packets.
- disable - Disables snooping system sparse mode in the switch. Floods unknown multicast packets.

Mode Global Configuration Mode

Default disable

Note: Sparse mode is in enabled state only when the snooping mode is set as MAC Based

Example

```
Your Product(config)# ip igmp snooping sparse-mode enable
```

Related Command(s) `show ip igmp snooping globals` – Displays the IGMP snooping information for all VLANs or a specific VLAN.

snooping report-process config-level

Command Objective This command sets the configuration-level for report processing as non-router ports or as all ports.

Syntax **snooping report-process config-level {non-router-ports | all-ports}**

Parameter Description

- `non-router-ports` - The incoming report messages are processed only in the non-router ports. Report message received on the router ports are not processed in this configuration.
- `all-ports` - The incoming report messages are processed in all the ports inclusive of router ports.

Mode Global Configuration Mode

Default non-router-ports

Example Your Product(config)# snooping report-process config-level all-ports

Related Command(s) `show ip igmp snooping globals` - Displays the IGMP snooping information for all VLANs or a specific VLAN.

ip igmp snooping multicast-vlan

Command Objective This command configures the multicast VLAN feature on a port. Multicast VLAN feature is used for applications where wide-scale deployment of multicast traffic is necessary. MVLAN registration allows a subscriber on a port to subscribe and unsubscribe to a particular multicast stream on any of the multicast VLANs. Multicast VLANs enable efficient multicast data flow in separate M-VLANs, while normal data flows through VLANs.

Syntax **ip igmp snooping multicast-vlan {enable|disable}**

Parameter Description

- `enable` - Enables the multicast Vlan feature. Router sends a single copy of the data for the particular MVLAN, instead of forwarding a separate copy of the multicast data to each VLAN. This saves the network bandwidth
- `disable` - Disables the multicast Vlan feature. A separate copy of the multicast data has to be forwarded from the router in the absence of M- VLAN.

Mode Global Configuration Mode

Default disable

Example `Your Product(config)# ip igmp snooping multicast-vlan enable`

Related Command(s)

- `show ip igmp snooping multicast-vlan` – Displays multicast VLAN statistics in a switch and displays various profiles mapped to the multicast VLANs.
- `show ip igmp snooping globals` – Displays IGMP snooping information for all VLANs or a

mvr

Command Objective This command configures the multicast VLAN feature on a port. Multicast VLAN feature is used for applications where wide-scale deployment of multicast traffic is necessary. MVLAN Registration allows a subscriber on a port to subscribe and unsubscribe to a particular multicast stream on any of the multicast VLANs. Multicast VLANs enable efficient multicast data flow in separate M-VLANs, while normal data flows through VLANs.

The no form of this command disables the multicast VLAN feature.

This command is a standardized implementation of the existing command; ip igmp snooping multicast-vlan. It operates similar to the existing command.

Syntax **mvr**

no mvr

Mode Global Configuration Mode

Package Workgroup, Enterprise, Metro_E and Metro

Example `Your Product(config)# mvr`

Related Command(s)

- `show ip igmp snooping multicast-vlan` – Displays multicast VLAN statistics in a switch and displays various profiles mapped to the multicast VLANs

- `show ip igmp snooping globals` – Displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switch (if switch is not specified)

ip igmp snooping filter

Command Objective This command configures the IGMP snooping filter. The IGS filtering feature restricts channel registration from being added to the database. In transparent snooping, the filtered packet will not be added to the snooping database but will be forwarded upstream. When disabled, all the filter related configurations remain but the incoming reports will not be subject to filtering. IGS module programs the hardware to remove the configured rate limit. It flushes all the registrations learnt through a port if a threshold limit is configured for this interface.

The no form of the command disables the IGMP snooping filter.

Syntax **ip igmp snooping filter**
no ip igmp snooping filter

Mode Global Configuration Mode

Default disabled.

Example Your Product(config)# ip igmp snooping filter

Related Command(s)

- `show ip igmp snooping globals` – Displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switch (if switch is not specified).
- `ip igmp snooping ratelimit` – Configures the rate limit for a downstream interface in units of the number of IGMP packets per second.
- `ip igmp snooping limit` – Configures the maximum limit type for an interface.
- `ip igmp snooping filter-profileId` – Configures the multicast profile index for a downstream interface.

ip igmp snooping blocked-router

Command Objective This command configures a static router-port as blocked router port. When configured as a blocked router, the queries, PIM DVMRP and data messages are discarded, The corresponding port entry is removed from the forwarding database. The ports to be configured as blocked router ports, must not be configured as static router ports.

The no form of the command resets the blocked router ports to normal router port.

Syntax **ip igmp snooping blocked-router <interface-type> <0/a-b,0/c, ...>**

no ip igmp snooping blocked-router <interface-type> <0/a- b, 0/c, ...>

Parameter Description

- `<interface-type>` - Configures the type of interface to be employed on the port.
  - `qx-ethernet` – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<0/a-b, 0/c, ...>` - Configures the list of router-ports to be set as blocked. The interface ids are given as an array. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel.Use comma as a separator without space while configuring list ofinterfaces. Example: 0/1, 0/3 or 1, 3.

Mode Config-VLAN Mode

Note: The ports to be configured as blocked router ports, must not be configured as static router ports.

Example

```
Your Product (config-vlan)# ip igmp snooping blocked-router gigabitethernet
0/4-5
```

Related Command(s) `show ip igmp snooping blocked-router` – Displays the blocked router ports for all VLANs or a specific VLAN for a given switch or for all the switches (if no switch is specified)

ip igmp snooping multicast-vlan profile

Command Objective This command configures profile ID to VLAN mapping for multicast VLAN classification. The switch is configured with list of entries such as multicast group, multicast source and filter mode. These entries are maintained in access profiles. Each profile is associated with a particular vlan which is categorized as multicast vlan. When any untagged report or leave message is received (that is, packet with no tag in a customer bridge or packet with no S-tag in a provider or 802.1ad bridge), and if the group and source address in the received packet matches any rule in this profile, then the received packet is classified to be associated to the VLAN (that is, multicast VLAN) to which the profile is mapped.

The no form of the command removes the profile ID to VLAN mapping for multicast VLAN classification.

Syntax **ip igmp snooping multicast-vlan profile <Profile ID (0-4294967295)>**

no ip igmp snooping multicast-vlan profile

Parameter Description `<Profile ID (0-4294967295)>` - Configures the multicast profile ID for a particular VLAN. This value ranges between 0 and 4294967295.

Mode Config-VLAN Mode

Default 0

Notes:

- Multicast snooping mode should be IP based.
- This command can be executed only after creating a multicast profile and setting the action for the created profile as permit.
- The configurations done by this command will take effect only if the profile is activated.

Example

```
Your Product (config-vlan)# ip igmp snooping multicast-vlan profile 1
```

Related Command(s)

- `ip mcast profile` – Creates or modifies a multicast profile.
- `permit`– Configures the action for the profile as permit.
- `profile active` – Activates the profile entry.
- `show ip mcast profile statistics` – Displays the profile statistics.

ip igmp snooping leavemode

Command Objective This command configures the port leave mode for an interface. The mechanism to process the leave messages in the downstream is selected. The switch sends an IGMP query message to find if there is any host interested in the multicast group.

Syntax **ip igmp snooping leavemode {exp-hosttrack | fastLeave | normalleave} [InnerVlanId <short (1-4094)>]**

Parameter Description

- `exp-hosttrack` - Configures the port to use the explicit host tracking mode to process the leave messages. The decision to remove the interface is made based on the tracked host information
- `fastLeave` - Configures the port to use the fast leave mode to process the leave messages. On receiving a leave message, the interface is removed from the group registration and the leave message is sent to the router ports.
- `normalleave` - Configures the port to use the normal leave mode. The normal leave mode is applicable only for v2 hosts. When the system receives a v2 leave message, it sends a group specific query on the interface. For v3 hosts normal leave has no effect.
- `innerVlanId <short (1-4094)>]` - Configures the inner vlan Id. In provider bridging domain, the customer vlan itag is denoted as innervlan id. This value ranges between 1 and 4094.
    - If InnerVlanId is specified, multicast forwarding mode must be IP based and enhanced mode must be enabled in the snooping system,
    - If InnerVlanId is not specified, leave mode can be configured irrespective of multicast

forwarding mode and enhanced mode status.

Mode Interface configuration mode

Package Workgroup, Enterprise, Metro_E and Metro

Default exp-host track/fastLeave/normalleave - Normalleave

Example

```
Your Product(config-if)# ip igmp snooping leavemode fastLeave InnerVlanId 1
```

Related Command(s)

- `snooping leave-process config-level` – Specifies the level of configuring the leave processing mechanisms
- `ip igmp snooping enhanced-mode` – Enables/disables snooping system enhanced mode in the switch.
- `snooping multicast-forwarding-mode` – Specifies the snooping multicast forwarding mode.
- `show ip igmp snooping port-cfg` – Displays IGS Port configuration information for all Inner VLANs or a specific Inner VlanId or a given switch.
- `show ip igmp snooping multicast-receivers` – Displays IGMP multicast host information for all VLANs or a specific VLAN or specific VLAN and group address for a given switch or for all switches (if no switch is specified).

ip igmp snooping ratelimit

Command Objective This command configures the rate limit for a downstream interface in units of the number of IGMP packets per second. The switch allows to configure the maximum rate of IGMP reports incoming for a port. The IGMP rate limiting eliminates the bursts or attacks from specific physical port. It prevents the exhaustion of system resources.

The no form of the command resets the rate limit to default value for an interface. By default, the rate limit will hold the maximum value supported by an unsigned integer and will not rate limit any IGMP packets.

Syntax **ip igmp snooping ratelimit <integer> [InnerVlanId <short (1-4094)>]**

no ip igmp snooping ratelimit [InnerVlanId <short (1-4094)>]

Parameter Description

- ratelimit <integer> - Configures the ratelimit value for a downstream interface in units of the number of IGMP packets per second
- InnerVlanId <short (1-4094)> - Configures the ratelimit value for Inner VLAN identifier. This value ranges between 1 and 4094. If InnerVlanId is specified, then enhanced mode should be enabled otherwise enhanced mode need not be enabled

Mode Interface configuration mode

Default rate limit is 4294967295.

Notes:

- The actual rate supported will depend on what the system can support.
- The IGMP snooping filter must be enabled for this configuration to have the effect.
- Even with out enabling IGMP snooping filter, control plane data structure update takes place. But the benefits can be realized only when IGMP Snooping filter is enabled.

Example

```
Your Product(config-if)# ip igmp snooping ratelimit 100 InnerVlanId 1
```

Related Command(s)

- `ip igmp snooping enhanced-mode` – Enables/disables snooping system enhanced mode in the switch.
- `ip igmp snooping filter` – Enables the IGMP snooping filter.
- `show ip igmp snooping port-cfg` – Displays IGS Port configuration information for all Inner VLANs or a specific Inner VlanId or a given switch.
- `ip mcast profile` – Creates or modifies a multicast profile.
- `profile active` – Activates the profile entry.

ip igmp snooping limit

Command Objective This command configures the maximum limit type for an interface. The maximum limit is the number of unique registrations for a channel or group.

The no form of the command configures the maximum limit type as none for an interface.

Syntax **ip igmp snooping limit { channels | groups } <interger32> [InnerVlanId <short (1-4094)>]**

no ip igmp snooping limit [InnerVlanId <short (1-4094)>]

Parameter Description

- `Channels` - Configures the snooping maximum limit as channels (group, source).Channel limit is applied for IGMPv3 include and allow reports.
- `Groups` - Configures the snooping maximum limit as groups. Group limit is applied for all IGMP reports.
- `<interger32>` - Configures the snooping maximum limit. The maximum limit is the number of unique registrations for a channel or group. This value ranges between 0 and 4294967295.
- `InnerVlanId <short (1-4094)>` - Configures the maximum limit type for the Inner VLAN identifier. This value ranges between 1 and 4094. If InnerVlanId is specified, then enhanced mode should be enabled otherwise enhanced mode need not be enabled.

Mode Interface configuration mode

Default The limit is set as 0 so that no limiting is done.

Notes:

- The IGMP snooping filter must be enabled for this configuration to have the effect.
- Even without enabling IGMP snooping filter, control plane data structure update takes place. But the benefits can be realized only when IGMP Snooping filter is enabled.

Example `Your Product(config-if)# ip igmp snooping limit groups 10 InnerVlanId 1`

Related Command(s)

- `ip igmp snooping enhanced-mode` – Enables/disables snooping system enhanced mode in the switch.
- `ip igmp snooping filter` – Enables the IGMP snooping filter.
- `show ip igmp snooping port-cfg` – Displays IGS Port configuration information for all Inner VLANs or a specific Inner VlanId or a given switch.
- `ip mcast profile` – Creates or modifies a multicast profile.
- `profile active` – Activates the profile entry.

ip igmp snooping filter-profileId

Command Objective This command configures the multicast profile index for a downstream interface. This profile contains a set of allowed or denied rules to be applied for the IGMP packets received through this downstream interface.

The no form of the command resets the multicast profile index to default value.

Syntax **ip igmp snooping filter-profileId <integer> [InnerVlanId <short (1-4094)>]**

no ip igmp snooping filter-profileId [InnerVlanId <short (1-4094)>]

Parameter Description

- `filter-profileId <integer>` - Configures the multicast filter profile index for a downstream interface.
- `InnerVlanId <short (1-4094)>` - Configures multicast filter profile index for the Inner VLAN identifier. This value ranges between 1 and 4094. If InnerVlanId is specified, then enhanced mode should be enabled otherwise enhanced mode need not be enabled.

Mode Interface configuration mode

Default The profile ID is 0.

Notes:

- The IGMP snooping filter must be enabled for this configuration to have the effect.
- Even without enabling IGMP snooping filter, control plane data structure update takes place. But the benefits can be realized only when IGMP Snooping filter is enabled.
- IGMP Snooping Multicast forwarding mode must be IP based.

Example `Your Product(config-if)# ip igmp snooping filter-profileId 2 InnerVlanId 1`

Related Command(s)

- `ip igmp snooping enhanced-mode` – Enables/disables snooping system enhanced mode in the switch.
- `ip igmp snooping filter` – Enables the IGMP snooping filter.
- `snooping multicast-forwarding-mode ip` - Sets the snooping multicast forwarding mode as IP address based.
- `show ip igmp snooping port-cfg` – Displays IGS Port configuration information for all Inner VLANs or a specific Inner VlanId or a given switch.
- `ip mcast profile` – Creates or modifies a multicast profile.
- `profile active` – Activates the profile entry.
- `show ip mcast profile statistics` – Displays the profile statistics.

ip igmp snooping proxy

Command Objective This command enables proxy in the IGMP snooping switch. In proxy mode, the switch acts as a querier for all downstream interfaces and a host for all upstream interfaces. The switch sends general query to all downstream interfaces at the query interval and collects information about the member ports. The proxy sends current consolidated report and state change report to upstream interfaces.

The no form of the command disables proxy in the IGMP snooping switch.

Syntax **ip igmp snooping proxy**

no ip igmp snooping proxy

Mode Global Configuration Mode

Default The proxy is disabled in the IGMP snooping switch.

Note: Proxy can be enabled in the IGMP snooping switch only if the proxy reporting is disabled in the snooping switch.

Example Your Product(config)# ip igmp snooping proxy

Related Command(s)

- no ip igmp snooping proxy-reporting – Disables proxy reporting in the IGMP snooping switch.

- show ip igmp snooping globals – Displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switch (if switch is not specified).

ip igmp snooping max-response-code

Command Objective This command sets the maximum response code inserted in general queries sent to host. The unit of the response code is tenth of second. This value ranges between 0 and 255.

The no form of the command sets the query response code to default value.

Syntax **ip igmp snooping max-response-code <(0 - 255)>**

no ip igmp snooping max-response-code

Mode Config-VLAN Mode

Default 100

Example Your Product(config-vlan)# ip igmp snooping max-response- code 10

Related Command(s) `show ip igmp snooping` - Displays IGMP snooping information for all VLANs or a specific VLAN.

ip igmp snooping mrouter-port –time-out

Command Objective This command configures the router port purge time-out interval for a VLAN. The time interval after which the proxy assumes there are no v1/v2 routers present on the upstream port. While the older querier timer is running, the proxy replies to all the queries with consolidated v1/v2 reports. When the timer expires, if the v2/v3 queriers are not present and the port is dynamically learnt, the port is purged. If the port is static, router port, the proxy replies to all queries with new version of v2/v3 consolidated reports.

The no form of the command resets the router port purge time-out interval to default, for a VLAN.

Syntax **ip igmp snooping mrouter-port <ifXtype> <iface_list> time- out <short(60-600)>**

no ip igmp snooping mrouter-port <interface-type> <0/a-b,0/c, ...>

Parameter Description

- `<ifXtype> / <interface-type>` - Configures the purge time-out interval for the specified type of interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

- `extreme-ethernet` **–** A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `port-channel` **–** Logical interface that represents an aggregator which contains several ports aggregated together.
- `<iface_list> / <0/a-b, 0/c, ...>` - Configures the list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel. Use comma as a separator without spacewhile configuring list of interfaces. Example: 0/1, 0/3 or 1, 3.
- `time-out <short(60-600)>` - Configures the router port purge time- out interval. This value ranges between 60 and 600 seconds.

Mode Config-VLAN Mode

Default time-out - 125 seconds

Note: The router ports must be statically configured for the VLAN.

Example

```
Your Product(config-vlan)# ip igmp snooping mrouter-port gigabitethernet
0/1-3 time-out 150
```

Related Command(s)

- `ip igmp snooping mrouter` – Configures statically the router ports for a VLAN
- `show ip igmp snooping mrouter detail`– Displays detailed information about the router ports.

ip igmp snooping mrouter-port-version

Command Objective This command configures the operating version of IGMP PROXY on the upstream router port for a VLAN.

The no form of the command resets the operating version of the IGMP PROXY on the upstream router port to its default operating version.

Syntax **ip igmp snooping mrouter-port <ifXtype> <iface_list> version {v1 | v2 | v3}**

no ip igmp snooping mrouter-port <ifXtype> <iface_list> version

Parameter Description

- `<ifXtype>` - Configures the operating version of IGMP PROXY for the specified type of interface. The interface can be:
  - **qx-ethernet –** A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - **gigabitethernet –** A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.

    - **extreme-ethernet –** A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
    - **port-channel –** Logical interface that represents an aggregator which contains several ports aggregated together.
- `<iface_list>` - Configures the operating version of IGMP PROXY for the list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel. Use comma as a separator without spacewhile configuring list of interfaces. Example: 0/1, 0/3 or 1, 3.
- `Version` - Configures the operating version of the IGMP snooping
    - v1 **–** IGMP snooping Version1
    - v2 **–** IGMP snooping Version2
    - v3 **–** IGMP snooping Version3

Mode Config-VLAN Mode

Default v3

Note: The router ports must be statically configured for the VLAN.

Example

```
Your Product(config-vlan)# ip igmp snooping mrouter-port gigabitethernet
0/2 version v1
```

Related Command(s)

- `ip igmp snooping mrouter` – Configures statically the router ports for a VLAN.
- `show ip igmp snooping mrouter detail` – Displays detailed information about the router ports

show ip igmp snooping mrouter

Command Objective This command displays the router ports for all VLANs or a specific VLAN for a given switch or for all the switches (if no switch is specified). The interface details and the corresponding port number along with its type (static/dynamic are displayed.

Syntax **show ip igmp snooping mrouter [Vlan <vlan-id/vfi-id>] [detail] [switch <switch_name>]**

Parameter Description

- `Vlan <vlan-id/vfi-id>` - Displays the router ports for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
    - `<vlan -id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
    - `<vfi-id>.` - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This

value ranges between 4096 and 65535. This type of switch is not supported.

Notes:

- The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
- VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
- The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- `detail` - Displays detailed information about the router ports
- `switch <switch_name>` - Displays the router ports for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Single Instance
Your Product# show ip igmp snooping mrouter
Vlan  Ports
-------- ----------
    1 Gi0/1(dynamic), Gi0/2(static)
    2 Gi0/1(static), Gi0/2(dynamic)
Multiple Instance
Your Product# show ip igmp snooping mrouter
Switch cust1
Vlan  Ports
-------- ----------
    1 Gi0/1(static)
    2 Gi0/1(static) Switch cust2
Vlan  Ports
-------- ----------
    1 Gi0/9(static)
    2 Gi0/9(static)
```

Related Command(s)

- `ip igmp snooping mrouter-time-out / ip igmp querier- timeout` - Sets the IGMP snooping router port purge time-out interval
- `ip igmp snooping mrouter` - Configures statically the router ports for a VLAN.
- `ip igmp snooping mrouter-port -time-out` - Configures the router port purge time-out interval for a VLAN.
- `ip igmp snooping mrouter-port-version` - Configures the operating version of the router port for a VLAN.

show ip igmp snooping mrouter - Redundancy

Command Objective This command displays the router ports for all VLANs or a specific VLAN for a given switch or for all switches (if no switch is specified).

Syntax **show ip igmp snooping mrouter [Vlan <vlan-id/vfi-id>] [redundancy] [detail] [switch <switch_name>]**

Parameter Description

- Vlan <vlan-id/vfi-id> - Displays the router ports for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
    - <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
    - <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

      Notes:

        - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
        - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
        - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- `redundancy` - Displays the Synced Messages
- `detail` - Displays detailed information about the router ports
- `switch <switch_name>` - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip igmp snooping mrouter redundancy
Igs Redundancy Vlan Sync Data for Vlan 1
Vlan Router Port List
Vlan  Ports
-------- ----------
    1 Gi0/1(dynamic), Gi0/3(dynamic)
IGMP Router Port List
Vlan  IGMP Ports
-------- ----------------
```

```
    1 Gi0/1(dynamic)
```

Related Command(s)

- `ip igmp snooping mrouter` - Configures statically the router ports for a VLAN
- `ip igmp snooping mrouter-port -time-out` - Configures the router port purge time-out interval for a VLAN.
- `ip igmp snooping mrouter-port-version` - Configures the operating version of the router port for a VLAN.

show ip igmp snooping globals

Command Objective This command displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switches (if switch is not specified).

Syntax **show ip igmp snooping globals [switch <switch_name>]**

Syntax `switch <switch_name>` - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip igmp snooping globals
Snooping Configuration
---------------------------------------------
IGMP Snooping globally enabled
IGMP Snooping is operationally enabled
IGMP Snooping Enhanced mode is disabled
Transmit Query on Topology Change globally disabled
Multicast forwarding mode is MAC based
Proxy globally disabled
Proxy reporting globally enabled
Filter is disabled
Router port purge interval is 125 seconds
Port purge interval is 260 seconds
Report forward interval is 5 seconds
Group specific query interval is 2 seconds
Reports are forwarded on router ports
Group specific query retry count is 2
Multicast VLAN disabled
Leave config level is Vlan based
```

Related Command(s)

- `ip igmp snooping` - Enables IGMP snooping in the switch/a specific VLAN
- `ip igmp snooping proxy-reporting` - Enables proxy reporting in the IGMP snooping switch
- `snooping multicast-forwarding-mode` - Specifies the forwarding mode (IP based or MAC based) that will be effective on switch restart

- ip igmp snooping mrouter-port –time-out / ip igmp querier-timeout - Sets the IGMP snooping router port purge time-out interval
- ip igmp snooping port-purge-interval / ip igmp snooping source-only learning age-timer - Configures the IGMP snooping port purge time interval
- ip igmp snooping report-suppression interval - Sets the IGMP report-suppression interval
- ip igmp snooping retry-count - Sets the maximum number of group specific queries sent on a port on reception of a IGMPV2 leave message
- ip igmp snooping version – Specifies the IGMP snooping operating mode of the switch
- ip igmp snooping report-forward - Specifies if IGMP reports must be forwarded on all ports or router ports of a VLAN
- snooping leave-process config-level - Specifies the level of configuring the leave processing mechanisms.
- ip igmp snooping enhanced-mode - Enables/disables snooping system enhanced mode in the switch.
- ip igmp snooping multicast-vlan - Enables/disables the multicast VLAN feature.
- mvr - Enables the multicast VLAN feature. This command is applicable only for the code using industry standard commands
- ip igmp snooping filter - Enables the IGMP snooping filter.
- ip igmp snooping proxy – Enables proxy in the IGMP snooping switch.
- ip igmp snooping send-query - Configures the IGMP general query transmission feature.

show ip igmp snooping

Command Objective This command displays IGMP snooping information for all VLANs or a specific VLAN for a given context or for all the contexts (if no switch is specified).

Syntax **show ip igmp snooping [Vlan <vlan-id/vfi-id>] [switch<switch_name>]**

Parameter Description

- Vlan <vlan-id/vfi-id> - Displays IGMP snooping information for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
    - <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
    - <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

    Notes:

        - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
        - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
        - The theoretical maximum for the maximum number of VFI is 65535 but the actual

number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- `switch <switch_name>` - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip igmp snooping vlan 2
Snooping VLAN Configuration for the VLAN 1
IGMP Snooping enabled
IGMP configured version is V3
Fast leave is disabled
Snooping switch is acting as Non-Querier
Query interval is 125 seconds
Port Purge Interval is 260 seconds
Max Response Code is 100, Time is 10 seconds
```

Related Command(s)

- `ip igmp snooping` - Enables IGMP snooping in the switch/a specific VLAN
- `ip igmp snooping version` - Specifies the IGMP snooping operating mode of switch
- `ip igmp snooping port-purge-interval / ip igmp snooping source-only learning age-timer` - Configures the IGMP snooping port purge time interval
- `ip igmp snooping fast-leave / ip igmp snooping vlan – immediate leave` - Enables fast leave processing and IGMP snooping for a specific VLAN
- `ip igmp snooping querier` - Configures the IGMP snooping switch as a querier for a specific VLAN
- `ip igmp snooping query-interval` - Sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN
- `ip igmp snooping max-response-code` - Sets the maximum response code inserted in general queries send to host.

show ip igmp snooping - Redundancy

Command Objective This command displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switches (if no switch is specified).

Syntax **show ip igmp snooping [Vlan <vlan-id/vfi-id>] [redundancy] [switch <switch_name>]**

Parameter Description

- `Vlan <vlan-id/vfi-id>` - Displays IGMP snooping information for the specified VLAN / VFI ID.

This value ranges between 1 and 65535.

  - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - `<vfi-id>.` - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

    Notes:

    - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
    - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
    - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- `redundancy` - Displays the Synced Messages
- `switch <switch_name>` - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip igmp snooping redundancy
IGMP Snooping VLAN Configuration for VLAN 1
IGMP snooping switch is acting as Non-Querier
IGMP current operating version is V1
```

Related Command(s)

- `ip igmp snooping` - Enables IGMP snooping in the switch/a specific VLAN
- `ip igmp snooping version` - Specifies the IGMP snooping operating mode of switch
- `ip igmp snooping fast-leave / ip igmp snooping vlan – immediate leave` - Enables fast leave processing and IGMP snooping for a specific VLAN
- `ip igmp snooping querier` - Configures the IGMP snooping switch as a querier for a specific VLAN
- `ip igmp snooping query-interval` - Sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN

show ip igmp snooping groups

Command Objective This command displays IGMP group information for all VLANs or a specific VLAN or specific VLAN and group address for a given switch or for all switch (if no switch is specified) . It also displays the information for static / dynamic or both types of multicast entries.

Syntax **show ip igmp snooping groups [Vlan <vlan-id/vfi-id> [Group<Address>]][{static | dynamic}][switch <switch_name>]**

Parameter Description

- `Vlan <vlan-id/vfi-id>` - Displays IGMP snooping group information for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
    - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
    - `<vfi-id>`. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

      Notes:

        - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
        - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
        - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- `Group <Address>` - Displays the Group Address of the VLAN ID
- `static` - Displays only static multicast entries
- `dynamic` - Displays only dynamic multicast entries. If not specified, both static and dynamic entries are displayed
- `switch <switch_name>` - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

Single Instance

/* IP based */

```
Your Product# show ip igmp snooping groups
IGMP Snooping Group information
-----------------------------------------------
VLAN ID:2 Group Address: 227.1.1.1
Filter Mode: EXCLUDE Exclude sources: None V1/V2 Receiver Ports:
```

```
Gi0/4
V3 Receiver Ports: Port Number: Gi0/2
Include sources: None
Exclude sources:
12.0.0.10, 12.0.0.20
Port Number: Gi0/3
Include sources: None
Exclude sources:
12.0.0.40, 12.0.0.30
```

/* MAC based */

```
Your Product# show ip igmp snooping groups
IGMP Snooping Group information
------------------------------------------------
VLAN ID:2 Group Address: 227.1.1.1
Filter Mode: EXCLUDE Exclude sources: None Receiver Ports:
Gi0/2, Gi0/3, Gi0/4, Gi0/5
```

Related Command(s) `ip igmp snooping static-group` - Configure IGMP snooping static multicast for Vlan(s)

show ip igmp snooping forwarding-database

Command Objective This command displays multicast forwarding entries for all VLANs or a specific VLAN for a given switch or for all switches (if no switch is specified). It also displays the information for static / dynamic or both types of multicast entries.

Syntax **show ip igmp snooping forwarding-database [Vlan <vlan- id/vfi-id>] [{static | dynamic}] [switch <switch_name>]**

Parameter Description

- `Vlan <vlan-id/vfi-id>` - Displays multicast forwarding entries for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
    - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
    - `<vfi-id>`. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

      Notes:

        - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
        - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
        - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100

VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- `Static` - Display the static multicast forwarding entries.
- `Dynamic` - Display the dynamic multicast forwarding entries. If not specified, both static and dynamic entries are displayed
- `switch <switch_name>` - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

Single Instance

/* IP based */

```
Your Product# show ip igmp snooping forwarding-database static
Vlan Source Address Group Address Ports
-------------------------------------  ------------------------------------------------
2                        12.0.0.10227.1.1.1    Gi0/1, Gi0/3,Gi0/4
2                        12.0.0.20227.1.1.1    Gi0/1, Gi0/3,Gi0/4
2                        12.0.0.30227.1.1.1    Gi0/1, Gi0/2,Gi0/4
2                        12.0.0.40227.1.1.1    Gi0/1, Gi0/2,Gi0/
```

/* MAC based */

```
Your Product# show ip igmp snooping forwarding-database
Vlan MAC-Address         Ports
------- ---------------------------   --------
2 01:00:5e:01:01:01  Gi0/2, Gi0/3, Gi0/4, Gi0/5
2 01:00:5e:02:02:02   Gi0/2, Gi0/3
```

Related Command(s)

- ip igmp snooping - Enables IGMP snooping in the switch/a specific VLAN
- ip igmp snooping proxy-reporting – Enables proxy reporting in the IGMP snooping switch
- ip igmp snooping version - Configures the operating version of the IGMP snooping switch for a specific VLAN
- ip igmp snooping static-group - Configure IGMP snooping static multicast for Vlan(s) By default, both static and dynamic entries are displayed

show ip igmp snooping forwarding-database - Redundancy

Command Objective This command displays multicast forwarding entries for all VLANs or a specific VLAN for a given switch or for all switches (if no switch is specified). It also displays the information for static / dynamic or both types of multicast entries.

Syntax **show ip igmp snooping forwarding-database [Vlan <vlan- id/vfi-id>] [{static | dynamic}] [redundancy] [switch<switch_name>]**

Parameter Description

- Vlan <vlan-id/vfi-id> - Displays multicast forwarding entries for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

    Notes:

    - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
    - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
    - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- static - Display the static multicast forwarding entries.
- dynamic - Display the dynamic multicast forwarding entries. If not specified, both static and dynamic entries are displayed
- redundancy - Displays the Synced Messages.
- switch <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip igmp snooping forwarding-database redundancy
Igs Redundancy Multicast Group Info Sync Data
Vlan                     Group Address   Ports
----                     -------------   -----
1                        224.1.1.1Gi0/2, Gi0/3
1                        224.1.2.3Gi0/1, Gi0/3
```

Related Command(s)

- ip igmp snooping - Enables IGMP snooping in the switch/a specific VLAN
- ip igmp snooping proxy-reporting – Enables proxy reporting in the IGMP snooping switch

- `ip igmp snooping version` - Configures the operating version of the IGMP snooping switch for a specific VLAN
- `ip igmp snooping static-group` - Configure IGMP snooping static multicast for Vlan(s) By default, both static and dynamic entries are displayed

show ip igmp snooping statistics

Command Objective This command displays IGMP snooping statistics for all VLANs or a specific VLAN for a given switch or for all switches (if no switch is specified).

Syntax **show ip igmp snooping statistics [Vlan <vlan-id/vfi-id>] [switch <switch_name>]**

Parameter Description

- `Vlan <vlan-id/vfi-id>` - Displays IGMP snooping statistics for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - `<vfi-id>`. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

    Notes:

    - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
    - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
    - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- `switch <switch_name>` - Displays the IGMP snooping statistics for specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip igmp snooping statistics
IGMP Snooping Statistics for VLAN 1

IGMP Snooping General queries received : 3
IGMP Snooping Group specific queries received : 0
IGMP Snooping Group and source specific queries received : 0
IGMP Snooping V1/V2 reports received : 10
IGMP Snooping V3 reports received : 0
IGMP Snooping V3 IS_INCLUDE messages received : 0
IGMP Snooping V3 IS_EXCLUDE messages received : 0
IGMP Snooping V3 TO_INCLUDE messages received : 0
IGMP Snooping V3 TO_EXCLUDE messages received : 0
IGMP Snooping V3 ALLOW messages received : 0
IGMP Snooping V3 Block messages received : 0
IGMP Snooping V2 Leave messages received : 0
IGMP Snooping General queries transmitted : 0
IGMP Snooping Group specific queries transmitted : 2
IGMP Snooping V1/V2 reports transmitted : 0
IGMP Snooping V3 reports transmitted : 3
IGMP Snooping V2 leaves transmitted : 0
IGMP Snooping Packets dropped : 1
```

Related Command(s) `ip igmp snooping` - Enables IGMP snooping in the switch/a specific VLAN

show ip igmp snooping blocked-router

Command Objective This command displays the blocked router ports for all VLANs or a specific VLAN for a given switch or for all the switches (if no switch is specified).

Syntax **show ip igmp snooping blocked-router [Vlan <vlan-id/vfi- id>] [switch <switch_name>]**

Parameter Description

- `Vlan <vlan-id/vfi-id>` - Displays the blocked router ports for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
    - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
    - `<vfi-id>`. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

      Notes:

        - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
        - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
        - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- `switch <switch_name>` - Displays the blocked router ports for specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This

parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip igmp snooping blocked-router
Vlan Ports
------- --------
1    Gi0/1, Gi0/2, Gi0/3, Gi0/4
2     Gi0/6, Gi0/7, Gi0/8
```

Related Command(s) `ip igmp snooping blocked-router` – Configures statically the blocked router ports for a VLAN.

show ip igmp snooping multicast-receivers

Command Objective This command displays IGMP multicast host information for all VLANs or a specific VLAN or specific VLAN and group address for a given switch or for all switches (ifno switch is specified).

Syntax **show ip igmp snooping multicast-receivers [Vlan <vlan- id/vfi-id> [Group <Address>]] [switch <switch_name>]**

Parameter Description

- `Vlan <vlan-id/vfi-id>` - Displays the displays IGMP multicast host information for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - `<vfi-id>.` - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

    Notes:

    - The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
    - VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
    - The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- `Group` - Displays IGMP multicast host information for the Multicast group address.
- `switch <switch_name>` - Displays IGMP multicast host information for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is

32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Notes:

- IGMP snooping must be enabled in the switch.
- The port leave mode for an interface must be set as exp-hosttrack Your Product# show ip igmp snooping multicast-receivers Snooping Receiver Information

Example

```
---------------------------------------------
VLAN ID: 1 Group Address: 225.0.0.10
Receiver Port: Gi0/2
Attached Hosts: 12.0.0.10
Exclude Sources: None
VLAN ID: 1 Group Address: 225.0.0.20
Receiver Port: Gi0/2
Attached Hosts: 12.0.0.20
Include Sources: 14.0.0.10
Receiver Port: Gi0/4
Attached Hosts: 12.0.0.40
Include Sources: 14.0.0.20
```

Related Command(s)

- `ip igmp snooping` - Enables IGMP snooping in the switch/a specific VLAN
- `ip igmp snooping leavemode exp-hosttrack` – Processes the leave messages using the explicit host tracking mechanism.

show ip igmp snooping port-cfg

Command Objective This command displays IGS Port configuration information for all Inner VLANs or a specific Inner VlanId or a given switch.

Syntax **show ip igmp snooping port-cfg [{interface <interface- type> <interface-id> [InnerVlanId vlan-id(1-4094)] | switch <switch_name>}]**

Parameter Description

- `interface<interface-type> <interface-id>` - Displays IGS Port configuration information for the the interface type and interface identifier. The details to be provided are:
  - `<interface-type>` - Sets the type of interface. The interface can be:
    - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
    - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

        - extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
    - <interface-id> - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan. Only i-lan ID is provided, for interface type i- lan.
- InnerVlanId vlan-id(1-4094) - Displays the IGS Port configuration information for the Inner VLAN identifier. This value ranges between 1 and 4094.
- switch <switch_name> - Displays the IGS Port configuration information for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip igmp snooping port-cfg
Snooping Port Configurations
-------------------------------------------
Snooping Port Configuration for Port 2
Leave Process mode is Normal Leave
Rate limit on the interface is 100
Max limit Type is Groups
Max limit is 20
Current member count is 0
Profile Id is 0
Snooping Port Configuration for Port 3
Leave Process mode is Fast Leave
Rate limit on the interface is -1
Max limit Type is Channels
Max limit is 500
Current member count is 0
Profile Id is 0
Your Product# show ip igmp snooping port-cfg interface gigabitethernet 0/2
Snooping Port Configurations
-------------------------------------------
Snooping Port Configuration for Port 2
Leave Process mode is Normal Leave
Rate limit on the interface is 100
Max limit Type is Groups
Max limit is 20
Current member count is 0
Profile Id is 0
```

Related Command(s)

- ip igmp snooping leavemode – Configures the port leave mode for an interface.
- ip igmp snooping ratelimit – Configures the rate limit for a downstream interface in units of the number of IGMP packets per second.
- ip igmp snooping limit – Configures the maximum limit type for an interface.
- ip igmp snooping filter-profileId – Configures the multicast profile index for a downstream

interface.

show ip igmp snooping multicast-vlan

Command Objective This command displays multicast VLAN statistics in a switch and displays various profiles mapped to the multicast VLANs.

Syntax **show ip igmp snooping multicast-vlan [switch<switch_name>]**

Parameter Description `switch <switch_name>` - Displays multicast VLAN statistics for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip igmp snooping multicast-vlan
Multicast VLAN Statistics
=========================
------------------------------------------------ Multicast VLAN disabled
Profile ID -- Multicast VLAN
------------------ ------
1      --
2       --
-------------------------------------------------------
```

Related Command(s)

- `ip igmp snooping multicast-vlan` – Enables/disables the multicast VLAN feature.
- `mvr` - Enables the multicast VLAN feature. This command is applicable only for the code using industry standard commands.

ip igmp snooping clear counters

Command Objective This command clears the IGMP snooping statistics maintained for Vlan(s).

Syntax **ip igmp snooping clear counters [Vlan <vlan-id/vfi-id>]**

Parameter Description

- Vlan <vlan-id/vfi-id> - Clears the IGMP snooping statistics maintained for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - `<vfi-id>`. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535. This interface type is not supported.

Notes:

- The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
- VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
- The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

Mode Global Configuration Mode

Example

```
Your Product(config)# ip igmp snooping clear counters vlan 4094
```

Related Command(s)

- `ip igmp snooping retry-count` - Sets the maximum number of group specific queries sent by the switch.
- `ip igmp snooping startup-query-count` - Sets the maximum number of general query messages sent out on switch startup, when the switch is configured as a querier.

ip igmp snooping send-query

Command Objective This command configures the IGMP general query transmission feature upon the topology change in the switch.

Syntax **ip igmp snooping send-query { enable | disable }**

Parameter Description

- `enable` - Enables the snooping query transmission status which generates IGMP query messages.
- `disable` - Disables the snooping query transmission status which stops the switch from generating IGMP query messages.

Mode Global Configuration Mode

Example

```
Your product(config)# ip igmp snooping send-query enable
```

Related Command(s) `show ip igmp snooping globals` - Displays IGMP snooping information for all/specified VLAN(s).

ip igmp snooping static-group

Command Objective This command configures IGMP snooping static multicast in the multicast switch

This no form of the command removes the IGMP snooping static multicast in the multicast switch

Syntax **ip igmp snooping static-group <mcast_addr> ports <ifXtype> <iface_list>**

no ip igmp snooping static-group <mcast_addr>

Parameter Description

- `<mcast_addr>` - Configures the Muticast Address. This value ranges between 225.0.0.0. and 239.255.255.255
- `<ifXtype>` - Configures snooping static multicast for the specified type of interface. The interface can be:
  - `qx-ethernet` – A version of Ethernet that supports data transfer up to 40 Gigabits per second. This Ethernet supports only full duplex links.
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `port-channel` – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<iface list>` - Configures snooping static multicast for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash, for interface type other than port-channel. Only port-channel ID is provided, for interface type port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3.

Mode Config-VLAN Mode

Example

```
Your Product (config-vlan)# ip igmp snooping static-group 225.3.2.2 ports
gigabitethernet 0/2
```

Related Command(s)

- `snooping multicast-forwarding-mode` - Specifies the snooping multicast forwarding mode
- `show ip igmp snooping forwarding - database static` – Displays static forwarding entries
- `show ip igmp snooping groups static` – Displays IGMP group information

25 RMON

RMON (Remote Monitoring) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data.

The RMON specification defines a set of statistics and functions that can be exchanged between RMON- compliant console managers and network probes. As such, RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.
The list of CLI commands for the configuration of RMON is as follows:

- set rmon
- rmon collection history
- rmon collection stats
- rmon event
- rmon alarm
- show rmon

set rmon

Command Objective This command is used to enable or disable the RMON feature.

Syntax **set rmon {enable | disable}**

Parameter Description

- `enable` - Enables the RMON feature in the system. On enabling, the RMON starts monitoring the networks both local and remote and provides network fault diagnosis
- `disable` - Disables the RMON feature in the system. On disabling, the RMON's network monitoring is called off.

Mode Global Configuration Mode

Default Disabled

Example

```
Your Product(config)# set rmon enable
```

Related Command(s) `show rmon` - Displays the RMON statistics, alarms, events, and history configured on the interface

rmon collection history

Command Objective This command enables history collection of interface/ VLAN statistics in the buckets for the specified time interval.

The no form of the command disables the history collection on the interface/VLAN.

Syntax **rmon collection history <index (1-65535)> [buckets <bucket-number (1-65535)>] [interval <seconds (1-3600)>] [owner <ownername (127)>]**

no rmon collection history <index (1-65535)>

Parameter Description

- `<index (1-65535)>` - Identifies an entry in the history control table. Each such entry defines a set of samples at a particular interval for an interface on the device. This value ranges between 1 and 65535.
- `buckets<bucket-number (1-65535)>` - Configures the number of buckets desired for the RMON collection history group of statistics. This is the requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this History Control EntryThe polling cycle is the bucket interval where the interface statistics details are stored. This value ranges between 1 and 65535.
- `interval<seconds (1-3600)>` - Configures the time interval over which the data is sampled for each bucket. The value ranges between 1 and 3600.
- `owner<ownername (127)>`- Configures the name of the owner of the RMON group of statistics.

Mode Interface Configuration Mode / Config VLAN Mode

Default

- bucket number - 50
- interval - 1800 seconds

Note: In Config VLAN Mode, this command executes only if either VLAN is set as active or if the member ports are associated with the VLAN.

Example

Interface Configuration Mode

```
Your Product(config) interface gigabitethernet 0/1
Your Product(config-if)# rmon collection history 1 buckets
2 interval 20
Config VLAN Mode
Your Product(config) vlan 1
Your Product(config-vlan) rmon collection history 2
```

Related Command(s)

- vlan active - Activates a VLAN in the switch.
- ports- Configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN.
- show rmon - Displays the history collection for the configured bucket

rmon collection stats

Command Objective This command enables RMON statistic collection on the interface/ VLAN.

The no form of the command disables RMON statistic collection on the interface/ VLAN.

Syntax **rmon collection stats <index (1-65535)> [owner <ownername (127)>]**

no rmon collection stats <index (1-65535)>

Parameter Description

- `<index (1-65535)>` - Identifies an entryin the statistics table. This value ranges between 1 and 65535.
- `owner <ownername (127)>` - Configures the the name of the owner of the RMON group of statistics

Mode Interface Configuration Mode / Config VLAN Mode

Note: In Config VLAN Mode, this command executes only if either VLAN is set as active or if the member ports are associated with the VLAN.

Example

```
Interface Configuration Mode
Your Product(config) interface gigabitethernet 0/1
Your Product(config-if)# rmon collection stats 1
```

```
Config VLAN Mode
Your Product(config) vlan 1
Your Product(config-vlan) rmon collection stats 2
```

Related Command(s)

- `vlan active` - Activates a VLAN in the switch.
- `ports`- Configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN.
- `show rmon` - Displays the RMON collection statistics

rmon event

Command Objective This command adds an event to the RMON event table. The added event is associated with an RMON event number.

The no form of the command deletes an event from the RMON event table.

Syntax **rmon event <number (1-65535)> [description <event- description (127)>] [log] [owner <ownername (127)>] [trap<community (127)>]**

no rmon event <number (1-65535)>

Parameter Description

- `<number (1-65535)>`- Sets the number of events to be added in the event table. This value ranges between 1 and 65535.
- `description<event-description (127)>` - Provides a description for the event. This value is a string with a maximum length of 127.

- log - Creates an entry in the log table for each event.
- owner<ownername (127)> - Displays the entity that are configured this entry. This value is a string with a maximum value of 127.
- trap<community (127)> - Generates a trap, The SNMP community string is to be passed for the specified trap. This value is a string with a maximum value of 127.

Mode Global Configuration Mode

Example

```
Your Product(config)# rmon event 1 log owner aricent trap netman
```

Related Command(s)

- rmon alarm - Sets an alarm on a MIB object
- show rmon - Displays the RMON events (show rmon events)
- show snmp community - Configures the SNMP community details

rmon alarm

Command Objective This command sets an alarm on a MIB object. The Alarm group periodically takes statistical samples from variables in the probe and compares them to thresholds that have been configured.

The no form of the command deletes the alarm configured on the MIB object.

Syntax **rmon alarm <alarm-number> <mib-object-id (255)> <sample- interval-time (1-65535)> {absolute | delta} rising- threshold <value (0-2147483647)> [rising-event-number (1-65535)] falling-threshold <value (0-2147483647)> [falling- event-number (1-65535)] [owner <ownername (127)>]**

no rmon alarm <number (1-65535)>

Parameter Description

- <alarm-number>/ <number (1-65535)> - Displays the value of the statistic during the last sampling period. This value remains available until the current sampling period is completed. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This value is compared with the rising and falling thresholds. The value ranges between 1 and 65535.

- <mib-object-id (255)> - Identifies the mib object.

- <sample-interval-time (1-65535)> - Identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular level for a MIB object in the device. This value ranges between 1 and 65535 seconds.

- absolute - Compares the value of the selected variable with the thresholds at the end of the sampling interval.

- delta - Subtracts the value of the selected variable at the last sample from the current value, and the difference is compared with the thresholds at the end of the sampling interval.
- rising-threshold <value (0-2147483647)> - Configures the rising threshold value. If the startup alarm is set as Rising alarm or RisingOrFalling alarm and if the configured threshold value is reached, then an alarm is raised. When the current sampled value is greater than or equal to the configured Rising threshold, and the value at the last sampling interval is less than this configured threshold, a single event will be generated. The value ranges between 0 and 2147483647.
- <rising-event-number (1-65535)> - Raises the index of the event, when the Rising threshold is reached. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. This value ranges between 1 and 65535.
- falling-threshold <value (0-2147483647)> - Configures the falling threshold value. If the startup alarm is set as Falling alarm or RisingOrFalling alarm and if the configured threshold value is reached, then an alarm is raised. When the current sampled value is lesser than or equal to the configured Falling threshold, and the value at the last sampling interval is greater than this threshold, a single event will be generated. This value ranges between 0 and 2147483647
- <falling-event-number (1-65535)> - Raises the index of the event when the Falling threshold is reached. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. This value ranges between 1 and 65535.
- owner<ownername (127)> - Sets the entity that are configured this entry.

Mode Global Configuration Mode

Default By default, the least event number in the event table is assigned for the rising and falling threshold as its event number.

Notes:

- RMON events must have been configured
- RMON collection stats must be configured
- In SMIS, we cannot monitor all the mib objects through RMON. This will be applicable only to the Ethernet interfaces and VLANs

Example

```
Your Product(config)# rmon alarm 4
1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 2 absolute
rising-threshold 2 2 falling-threshold 1 2 owner Aricent
```

Related Command(s)

- `rmon collection stats` - Enables RMON statistic collection on the interface
- `rmon event` - Adds an event to the RMON event table

- `show rmon` - Displays the RMON alarms (show rmon alarms)

show rmon

Command Objective This command displays the RMON statistics, alarms, events, and history configured on the interface.

Syntax **show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events] [history [history-index (1-65535)] [overview]]**

Parameter Description

- `statistics` - Displays a collection of statistics for a particular Ethernet Interface. The probe for each monitored interface on this device measures the statistics.
- `alarms` - Displays the value of the statistic during the last sampling period. This value remains available until the current sampling period is completed.
- `events` - Generates events whenever an associated condition takes place in the device. The Conditions may be alarms. Alarms are generated when a sampled statistical variable value exceeds the defined threshold value. Alarm module calls events module
- `history` - Displays the history of the configured RMON
- `overview` - Displays only the overview of rmon history entries

Mode Privileged EXEC Mode

Example

```
Your Product# show rmon statistics
RMON is enabled
Collection 4 on Vlan 1 is active, and owned by monitor, Monitors Vlan 1 which has
Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
0 out FCS errors,
# of packets received of length (in octets):
64: 0, 65-127: 0, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0
Collection 45 on Gi0/1 is active, and owned by monitor, Monitors ifEntry.1.1 which has
Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
0 out FCS errors,
# of packets received of length (in octets):
64: 0, 65-127: 0, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518:
Collection 56 on Vlan 5 is active, and owned by monitor, Monitors Vlan 5 which has
Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
0 out FCS errors,
# of packets received of length (in octets):
64: 0, 65-127: 0, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0
Number of statistics collection on interface: 1
Number of statistics collection on Vlan    : 2
Your Product# show rmon
RMON is enabled
Your Product# show rmon history
RMON is disabled
Entry 1 is active, and owned by monitor Monitors ifEntry.1.2 every 1800 second(s)
Requested # of time intervals, ie buckets, is 50, Granted # of time intervals, ie
buckets, is 50,
Entry 4 is active, and owned by monitor
Monitors Vlan 40 every 1800 second(s)
Requested # of time intervals, ie buckets, is 50, Granted # of time intervals, ie
buckets, is 50,
Number of history collection on interface: 1
Number of history collection on Vlan    : 1
Your Product# show rmon events
RMON is enabled
Event 1 is active, owned by
Description is
Event firing causes nothing,
Time last sent is Aug 27 18:30:01 2009
Event 2 is active, owned by
Description is
Event firing causes nothing,
Time last sent is Aug 27 18:31:36 2009
Your Product# show rmon alarms
RMON is enabled
Alarm 4 is active, owned by Aricent
Monitors 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 every
2 second(s)
Taking absolute samples, last value was 3
Rising threshold is 2, assigned to event 2
Falling threshold is 1, assigned to event 2
On startup enable rising or falling alarm
Your Product# show rmon statistics 2 alarms events history
1
RMON is enabled
Collection 2 on Ex0/1 is active, and owned by monitor, Monitors ifEntry.1.1 which has
Received 5194 octets, 53 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
53 CRC alignment errors and 0 collisions.
# of packets received of length (in octets):
64: 0, 65-127: 53, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0
Alarm 4 is active, owned by Aricent
```

```
Monitors 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 every
2 second(s)
Taking absolute samples, last value was 3
Rising threshold is 2, assigned to event 2
Falling threshold is 1, assigned to event 2
On startup enable rising or falling alarm
Event 1 is active, owned by
Description is
Event firing causes nothing,
Time last sent is Aug 27 18:30:01 2009
Event 2 is active, owned by
Description is
Event firing causes nothing,
Time last sent is Aug 27 18:31:36 2009
Your Product# show rmon history overview
RMON is enabled
Entry 1 is active, and owned by monitor Monitors ifEntry.1.2 every 1800 second(s)
Requested # of time intervals, ie buckets, is 50, Granted # of time intervals, ie
buckets, is 50,
Entry 4 is active, and owned by monitor
Monitors Vlan 40 every 1800 second(s)
Requested # of time intervals, ie buckets, is 50, Granted # of time intervals, ie
buckets, is 50,
Number of history collection on interface: 1
Number of history collection on Vlan    : 1
```

Related Command(s)

- `set rmon` - Enables or disables the RMON feature
- `rmon collection history` - Enables history collection of interface/VLAN statistics in the buckets for the specified time interval
- `rmon collection stats` - Enables RMON statistic collection on the interface/VLAN
- `rmon event` - Adds an event to the RMON event table
- `rmon alarm` - Sets an alarm on a MIB object

26 RMON2

RMONv2 is an extension of the RMON that deals with the information at the physical and data link network levels to support monitoring and protocol analysis of LANs. RMONv2 adds support for network and application layer monitoring.
RMONv2 is a portable implementation of Remote Network Monitoring version 2. RMONv2 is implemented with nine RMON Mib groups. They are Protocol directory, Protocol distribution, Address Map, Network Layer Host, Network Layer Matrix, Application Layer Host, Application layer Matrix, User History collection and Probe configuration groups. RMONv2 provides extensions to four RMONv1 tables. They are: etherStats table, historyControl table, hostControl table and matrixControl table. RMON should be enabled for configuring the RMONv1 tables

The list of CLI commands for the configuration of RMON2 is as follows:

- rmon2
- debug rmon2

rmon2

Command Objective This command enables / disables RMON2 module in the switch. RMON2.lists the inventory of protocols, lists MAC address to network address bindings, tracks the amount of traffic between network addresses and so on. The default value is disabled.

Syntax **rmon2 {enable | disable}**

Parameter Description

- `enable` - Enables the RMON2 module in the switch. Resources are allocated to the module.
- `disable` - Disables the RMON2 module in the switch. Resources allocated are released back to the system.

Mode Global Configuration Mode

Default disabled

Example

```
Your Product(config)# rmon2 enable
```

debug rmon2

Command Objective This command configures various RMON2 debug trace messages.

The no form of the command disables the debug feature for RMON2 module. Debug facility captures events, errors and the level of severity of the traces and logs them in a file.

Syntax **debug rmon2 {[func-entry][func-exit][critical][mem- fail][debug] | [ALL]}**

no debug rmon2

Parameter Description

- `func-entry` - Generates Function Entry Trace messages. When a function is called in the RMON2 module, the details of the function are displayed in the trace message. The traces are captured for all the functions in RMON2.
- `func-exit` - Generates Function Exit Trace messages. When the system completes a function and exits, the details of the function exited is displayed in the trace messages. The traces are captured for all functions.
- `critical` - Generates Critical Trace messages. The errors that cause damage or malfunctioning of the system are displayed as critical traces.
- `mem-fail` - Generates Memory failure Trace messages. When there is a constraint for memory allocation when a fuction is initiated, the mem-fail trace is displayed.
- `debug` - Generates Debug Trace messages for less severe errors and events.
- `ALL` - Generates all kinds of trace messages mentioned above.

Mode Privileged EXEC Mode

Example

```
Your Product# debug rmon2 ALL
```

27 QoS

QoS (Quality of Service) defines the ability to provide different priorities to different applications, users or data flows or the ability to guarantee a certain level of performance to a data flow. QoS refers to resource reservation control mechanisms rather than the achieved service quality and specifies a guaranteed throughput level.

SMIS QoS provides a complete IP Quality of Service solution and helps in implementing service provisioning policies for applicationor customers, who desire to have an enhanced performance for their trafficon the Internet.

The list of CLI commands for the configuration of QoSX is as follows:

- shutdown qos
- qos
- priority-map
- class-map
- meter
- policy-map
- queue-type
- shape-template
- scheduler
- queue
- queue-map
- sched-hierarchy
- qos interface
- map
- match access-group
- set class
- meter-type
- set policy
- set meter
- set algo-type
- random-detect dp
- show qos global info
- show priority-map
- show class-map
- show class-to-priority-map

- show meter
- show policy-map
- show queue-template
- show shape-template
- show scheduler
- show queue
- show queue-map
- show sched-hierarchy
- show qos pbit-preference-over-Dscp
- show qos def-user-priority
- show qos meter-stats
- show qos queue-stats
- debug qos
- qos pbit-preference
- cpu rate limit queue
- show cpu rate limit

shutdown qos

Command Objective This command shuts down the QoS subsystem.

The no form of the command starts the QoS subsystem.

Syntax **shutdown qos**

no shutdown qos

Mode Global Configuration Mode

Defaults QoS subsystem is started and enabled by default.

Note:

- Resources required by QoS subsystem are allocated and QoS subsystem starts running, when started.
- All the MemPools used by the QoS subsystem will be released, when shutdown.

Example

```
Your Product(config)# shutdown qos
```

Related Command(s) `show qos global info` – Displays QoS related global configurations.

qos

Command Objective This command enables / disables the QoS subsystem.

Syntax **qos {enable | disable}**

Parameter Description

- `enable` - Enables the QoS subsystem
- `disable` - Disables the Qos subsystem

Mode Global Configuration Mode

Defaults Enabled

Note:

- QoS module programs the hardware and starts protocol operation, when set as enable.
- QoS module stops protocol operation by deleting the hardware configuration, when set as disable.

Example

```
Your Product(config)# qos enable
```

Related Command(s) `show qos global info` – Displays QoS related global configurations.

priority-map

Command Objective This command adds a Priority Map entry. Configures the priority map index for the incoming packet received over ingress Port/VLAN with specified incoming priority. This value ranges between 1 and 65535.

The no form of the command deletes a Priority Map entry.

Syntax **priority-map <priority-map-Id(1-65535)>**

no priority-map <priority-map-Id(1-65535)>

Mode Global Configuration Mode

Note: QoS subsystem should have been started.

Example

```
Your Product(config)# priority-map 1
Your Product(config-pri-map)#
```

Related Command(s) `show priority-map` – Displays the Priority Map entry.

class-map

Command Objective This command adds a Class Map entry. Configures an Index that enumerates the MultiField Classifier table entries. This value ranges between 1 and 65535.

The no form of the command deletes a Class Map entry.

Syntax **class-map <class-map-id(1-65535)>**

no class-map <class-map-id(1-65535)>

Mode Global Configuration Mode

Note: QoS subsystem should have been started.

Example

```
Your Product(config)# class-map 1
Your Product(config-cls-map)#
```

Related Command(s) `show class-map` – Displays the Class Map entry.

meter

Command Objective This command creates a Meter. Configures an Index that enumerates the Meter entries. This value ranges between 1 and 65535.

The no form of the command deletes a Meter.

Syntax **meter <meter-id(1-65535)>**

no meter <meter-id(1-65535)>

Mode Global Configuration Mode

Note: QoS subsystem should have been started.

Example

```
Your Product(config)# meter 1
Your Product(config-meter)#
```

Related Command(s) `show meter` – Displays the Meter entry.

policy-map

Command Objective This command creates a policy map. Configures an Index that enumerates the policy-map table entries. This value ranges between 1 and 65535.

The no form of the command deletes a policy map.

Syntax **policy-map <policy-map-id(1-65535)>**

no policy-map <policy-map-id(1-65535)>

Mode Global Configuration Mode

Note: QoS subsystem should have been started.

Example

```
Your Product(config)# policy-map 1
Your Product(config-ply-map)#
```

Related Command(s) `show policy-map` – Displays the Policy Map entry.

queue-type

Command Objective This command creates a Queue Template Type. This value ranges between 1 and 65535.

The no form of the command deletes a Queue Template Type.

Syntax **queue-type <Q-Template-Id(1-65535)>**

no queue-type <Q-Template-Id(1-65535)>

Mode Global Configuration Mode

Example

```
Your Product(config)# queue-type 1
Your Product(config-qtype)#
```

Related Command(s) `show queue-template` – Displays the Q Template and Random Detect configurations.

shape-template

Command Objective This command creates a Shape Template.

The no form of the command deletes a Shape Template.

Syntax **shape-template <integer(1-65535)> [cir <integer(1-10485760)>] [cbs <integer(0-10485760)>] [eir <integer(0-10485760)>] [ebs <integer(0-10485760)>]**

no shape-template <Shape-Template-Id(1-65535)>

Parameter Description

- `shape-template <integer(1-65535)>` - Configures the shape Template Table index. This value ranges between 1 and 65535.
- `cir<integer(1-10485760)` - Configures the Committed information rate for packets through the queue. This value ranges between 1 and 10485760. Cir should be less than eir
- `cbs<integer(0-10485760)>` - Configures the Committed burst size for packets through the queue.

This value ranges between a and 10485760

- `eir<integer(0-10485760)>` - Configures the Excess information rate for packets through the hierarchy. This value ranges between a and 10485760
- `ebs<integer(0-10485760)>` - Configures the Excess burst size for packets through the hierarchy. This value ranges between a and 10485760

Mode Global Configuration Mode

Example Your Product(config)# shape-template 1 cir 20 cbs 40 eir 50 ebs 40

Related Command(s) `show shape-template` – Displays the Shape Template configurations.

scheduler

Command Objective This command creates a Scheduler and configures the Scheduler parameters.

The no form of the command deletes a scheduler.

Syntax **scheduler <integer(1-65535)> interface <iftype> <ifnum> [sched-algo {strict-priority | rr | wrr | wfq | strict-rr | strict-wrr | strict-wfq | deficit-rr}] [shaper <integer(0-65535)>] [hierarchy-level <integer(0-10)>]**

no scheduler <Scheduler-Id(1-65535)> interface <iftype> <ifnum>

Parameter Description

- `scheduler-Id<integer(1-65535)>` - Scheduler identifier that uniquely identifies the scheduler in the system/egress interface. This value ranges between 1 and 65535.
- `iftype` - Interface type. Supports everything except port-channel
- `ifnum` - Interface number.
- `sched-algo` - Packet scheduling algorithm for the port. The algorithms are:
  - `strict-priority`– strictPriority.
  - `rr`– roundRobin.
  - `wrr`– weightedRoundRobin.
  - `wfg`– weightedFairQueing.
  - `strict-rr`– strictRoundRobin.
  - `strict-wrr`– strictWeightedRoundRobin.
  - `strict-wfg`– strictWeightedFairQueing.
  - `deficit-rr`– deficitRoundRobin.

  Note: wfq/strict-wfq/deficit-rr are not supported in some modes.
- `shaper<integer(0-65535)>` - Shaper identifier that specifies the bandwidth requirements for the

scheduler. This value ranges between 0 and 65535.
- hierarchy-level<integer(0-10)> - Depth of the queue/scheduler hierarchy. This value ranges between 0 and 10.

Mode Global Configuration Mode

Defaults

- sched-algo - strict-priority
- hierarchy-level - 0

Example

```
Your Product(config)# scheduler 1 interface
gigabitethernet 0/1 sched-algo rr shaper 1 hierarchy-level
1
```

Note: Shape template with the shaper id should have been created to specify the bandwidth requirements for the scheduler

Related Command(s)

- show scheduler – Displays the configured Scheduler.
- sched-hierarchy – Creates a Scheduler Hierarchy.
- show sched-hierarchy – Displays the configured hierarchy scheduler.
- shape-template – Creates a Shape Template.

queue

Command Objective This command creates a Queue and configures the Queue parameters.

The no form of the command deletes a Queue.

Syntax **queue <integer(1-65535)> interface <iftype> <ifnum> [qtype <integer(1-65535)>] [scheduler <integer(1-65535)>] [weight <integer(0-1000)>] [priority <integer(0-15)>] [shaper <integer(0-65535)>] [queue-type {unicast | multicast }]**

no queue <integer(1-65535)> interface <iftype> <ifnum>

Parameter Description

- queue<integer(1-65535)> - Queue identifier that uniquely identifies the queue in the system/port. This value ranges between 1 and 65535.
- iftype - Interface type. Supports everything except port-channel
- ifnum - Interface number.
- qtype<integer(1-65535)> - Queue Type identifier. This value ranges between 1 and 65535.
- scheduler<integer(1-65535)> - Scheduler identifier that manages the specified queue. This value ranges between 1 and 65535.

- `weight<integer(0-1000)>` - User assigned weight to the CoS queue. This value ranges between 0 and 1000.
- `priority<integer(0-15)>` - User assigned priority for the CoS queue. This value ranges between 0 and 15.
- `shaper<integer(0-65535)>` - Shaper identifier that specifies the bandwidth requirements for the queue. This value ranges between 0 and 65535.
- `unicast` - Unicast queue to store known unicast packets
- `multicast` - Multicast queue to store DLF, multicast, broadcast and mirrored packets

Mode Global Configuration Mode

Defaults

- weight - 0
- priority - 0
- Queue-type - Unicast

Example Your Product(config)# queue 1 interface giga 0/1 qtype 2 scheduler 1 weight 20 priority 10 shaper 1.

Notes:

- Scheduler identifier is unique relative to an egress interface.
- User assigned weights are used only when scheduling algorithm is a weighted scheduling algorithm.
- User assigned priority is used only when the scheduler uses a priority based scheduling algorithm.

Related Command(s)

- `queue-type` – Creates a Queue Template Type.
- `scheduler` – Creates a Scheduler and configures the Scheduler parameters.
- `shape-template` – Creates a Shape Template.
- `show queue` – Displays the configured Queues.

queue-map

Command Objective This command creates a Map for a Queue with Class or regenerated priority.

The no form of the command deletes a Queue map entry.

Syntax **queue-map { CLASS <integer(1-65535)> | regn-priority {vlanPri | ipTos | ipDscp | mplsExp | vlanDEI } <integer(0-63)> } [interface <iftype> <ifnum>] queue-id <integer(1-65535)>**

no queue-map { CLASS <integer(1-65535)> | regn-priority {vlanPri | ipTos | ipDscp | mplsExp | vlanDEI } <integer(0-63)> } [interface <iftype> <ifnum>]

Parameter Description

- `CLASS <integer(1-65535)>` - Input CLASS that needs to be mapped to an outbound queue. This value ranges between 1 and 65535.
- `regn-priority<integer(0-63)>` - Regenerated-priority type and regenerated-priority that needs to be mapped to an outbound queue. The types are
  - `vlanPri`– VLAN Priority.
  - `ipTos`– IP Type of Service.
  - `ipDscp`– IP Differentiated Services Code Point.
  - `mplsExp`– MPLS Experimental
  - `vlanDEI`– VLAN Drop Eligibility Indicator.
- `iftype` - Interface type. Supports everything except port-channel
- `ifnum` - Interface number.
- `queue-id <integer(1-65535)>` - Queue identifier that uniquely identifies a queue relative to an interface. This value ranges between 1 and 65535.

Mode Global Configuration Mode

Example

```
Your Product(config)# queue-map CLASS 1 interface giga 0/1 queue-id 1
```

Notes:

- CLASS should be zero while configuring RegenPriority specific Q.
- Regenerated-priority should be zero while configuring CLASS specific Queue.

Related Command(s) `show queue-map` – Displays the configured Queue map.

sched-hierarchy

Command Objective This command creates a Scheduler Hierarchy.

The no form of the command deletes a Scheduler Hierarchy.

Syntax **sched-hierarchy interface <iftype> <ifnum> hierarchy-level <integer(1-10)> sched-id <integer(1-65535)> {next-level- queue <integer(0-65535)> | next-level-scheduler <integer(0-65535)>} [priority <integer(0-15)>] [weight <integer(0-1000)>]**

no sched-hierarchy interface <iftype> <ifnum> hierarchy- level <integer(1-10)> sched-id <integer(1-65535)>

Parameter Description

- `iftype` - Interface type. Supports everything except port-channel
- `ifnum` - Interface number.

- `hierarchy-level <integer(1-10)>` - Depth of the queue/scheduler hierarchy.
- `sched-id <integer(1-65535)>` - Scheduler identifier.
    - `next-level-queue` – Next-level queue to which the scheduler output needs to be sent.
    - `next-level-scheduler` – Next-level scheduler to which the scheduler output needs to be sent.
- `priority <integer(0-15)` - Scheduler priority.
- `weight <integer(0-1000)>` - Scheduler weight.

Mode Global Configuration Mode

Defaults priority - 0

Example

```
Your Product(config)# sched-hierarchy interface giga 0/1 hierarchy-level 3
sched-id 1 next-level-queue 2 priority 5 weight 50
```

Notes:

- The priority is specified when the scheduler is connecting to any of the priorities (EF, AF, BE) of the next level strict-priority scheduler.
- The weight is specified if the scheduler is connecting to a WeightedFairQueing of another scheduler.

Related Command(s)

- `show scheduler` – Displays the configured Scheduler.
- `sched-hierarchy` – Creates a Scheduler Hierarchy.
- `show sched-hierarchy` – Displays the configured hierarchy scheduler.

qos interface

Command Objective This command sets the default ingress user priority for the port.

Syntax **qos interface <iftype> <ifnum> def-user-priority <integer(0-7)>**

Parameter Description

- `iftype` - Interface type
- `ifnum` - Interface number
- `def-user-priority <integer(0-7)>` - Default ingress user priority for the port

Mode Global Configuration Mode

Example

```
Your Product(config)# qos interface gigabitethernet 0/1 def-user-priority 3
```

Note: The default ingress user priority will be used to set priority for untagged packets.

Related Command(s) `show qos def-user-priority`– Displays the configured default ingress user priority for a port.

map

Command Objective This command adds a Priority Map Entry for mapping an incoming priority to a regenerated priority.

The no form of the command sets default value to the Interface, VLAN, and regenerated inner priority.

Syntax **map [interface <iftype> <ifnum>] [vlan <integer(1-4094)>] in-priority-type { vlanPri | ipTos | ipDscp | mplsExp | vlanDEI } in-priority <integer(0-63)> regen-priority <integer(0-63)> [regen-inner-priority <integer(0-7)>]**

no map { interface | vlan | regen-inner-priority }

Parameter Description

- `iftype` - Interface type
- `ifnum` - Interface number
- `vlan <integer(1-4094)>` - VLAN identifier. This value ranges between 1 and 4094.
- `in-priority-type` - Type of the incoming priority. The types are:
  - `vlanPri` **–** VLAN Priority.
  - `ipTos` **–** IP Type of Service.
  - `ipDscp` **–** IP Differentiated Services Code Point.
  - `mplsExp` **–** MPLS Experimental
  - `vlanDEI` **–** VLAN Drop Eligibility Indicator.
- `in-priority <integer(0-63)>` - Incoming priority value determined for the received frame. This value ranges between 0 and 63.
- `regen-priority <integer(0-63)>` - Regenerated priority value determined for the received frame. This value ranges between 0 and 63.
- `regen-inner-priority <integer(0-7)>` - Regenerated inner-VLAN (CVLAN) priority value determined for the received frame. This value ranges between 0 and 7.

Mode Priority Map Configuration Mode

Defaults

- vlan - 0
- in-priority-type - vlanPri
- in-priority - -1
- regen-priority - 0

Example

```
Your Product(config-pri-map)# map interface gig 0/1 vlan 4094 in-priority-type vlanPri
in-priority 0 regen-priority 7 regen-inner-priority 1
```

Note: Priority Map entry should have been created.

Related Command(s)

- `priority-map` – Adds a Priority Map entry
- `show priority-map` – Displays the Priority Map entry.

match access-group

Command Objective This command sets Class Map parameters using L2and/or L3 ACL or Priority Map ID.

Syntax **match access-group { [mac-access-list <integer(0-65535)>] [ip-access-list <integer(0-65535)>] | priority-map <integer(0-65535)> }**

Parameter Description

- `mac-access-list <integer(0-65535)>` - Identifier of the MAC filter. This value ranges between 0 and 65535.
- `ip-access-list <integer(0-65535)>` - Identifier of the IP filter. This value ranges between 0 and 65535.
- `priority-map <integer(0-65535)>` - Priority Map identifier for mapping incoming priority against received packet. This value ranges between 0 and 65535.

Mode Class Map Configuration Mode

Defaults

- mac-access-list - 0
- ip-access-list - 0
- priority-map - 0

Example

```
Your Product(config-cls-map)# match access-group priority-map 1
```

Notes:

- Priority map ID should have been created.
- L2 and/or L3 ACL should have been created.

Related Command(s)

- priority-map – Adds a Priority Map entry.
- show class-map – Displays the Class Map entry.

set class

Command Objective This command sets CLASS for L2and/or L3 filters or Priority Map ID and adds a CLASS to Priority Map entry with regenerated priority.

The no form of the command deletes a CLASS to Priority Map Table entry.

Syntax **set class <class integer(1-65535)> [pre-color { green | yellow | red | none }] [regen-priority <integer(0-7)> group-name <string(31)>]**

no set class <class integer(1-65535)>

Parameter Description

- `<class integer(1-65535)>` - Traffic CLASS to which an incoming frame pattern is classified.
- `pre-color` - Color of the packet prior to metering. This can be any one of the following:
    - `None`**–** Traffic is not pre-colored.
    - `green`**–** Traffic conforms to SLAs (Service Level Agreements.
    - `yellow`**–** Traffic exceeds the SLAs.
    - `red`**–** Traffic violates the SLAs.
- `regen-priority <integer(0-7)>` - Regenerated priority value determined for the input CLASS. This value ranges between 0 and 7.
- `group-name <string(31)>` - Unique identification of the group to which an input CLASS belongs.

Mode Class Map Configuration Mode

Defaults class - 0

Example

```
Your Product(config-cls-map)# set class 1000 pre-color none regen-priority
1 group-name CLASS
```

Notes:

- Class map should have created.
- The default value zero provided for the class is not configurable.

Related Command(s) `show class-to-priority-map` – Displays the class group Entry.

meter-type

Command Objective This command sets Meter parameters CIR, CBS, EIR, EBS, Interval, meter type and color awareness.

Syntax **meter-type { simpleTokenBucket | avgRate| srTCM | trTCM | tswTCM | mefCoupled | mefDeCoupled } [color-mode { aware | blind }] [interval <short(1-10000)>] [cir <integer(0-65535)>] [cbs <integer(0-65535)>] [eir <integer(0-65535)>] [ebs <integer(0-65535)>] [next-meter <integer(0-65535)>]**

Parameter Description

- simpleTokenBucket - Two Parameter Token Bucket Meter.
- avgRate - Average Rate Meter. Valid parameters supported are interval and cir. It is not supported in some models.
- srTCM - Single Rate Three Color Marker Metering as defined by RFC 2697. Valid parameters supported are cir, cbs and ebs
- trTCM - Two Rate Three Color Marker Metering as defined by RFC 2698. Valid value for Given Meter Type are CIR, CBS EIR, and EBS
- tswTCM - Time Sliding Window Three Color Marker Metering as defined by RFC 2859.
- mefCoupled - Dual bucket meter as defined by RFC 4115. It is not supported in some models.
- mefDeCoupled - Dual bucket meter as defined by RFC 2697 and MEF coupling Flag. It is not supported in some models.
- color-mode - Indicates the color mode of the Meter. The color modes are:
  - aware**–** The Meter considers the pre-color of the packet.
  - blind**–** The Meter ignores the pre-color of the packet.
- interval <short(1-10000)> - Time interval used with the token bucket. This value ranges between 1 and 10000.
- cir <integer(0-65535)> - Committed information rate. This value ranges between 0 and 65535.
- cbs <integer(0-65535)> - Committed burst size. This value ranges between 0 and 65535.
- eir <integer(0-65535)> - Excess information rate. This value ranges between 0 and 65535.
- ebs <integer(0-65535) - Excess burst size. This value ranges between 0 and 65535.
- next-meter <integer(0-65535)> - Meter entry identifier used for applying the second/next level of conformance on the incoming packet. This value ranges between 0 and 65535.

Mode Meter Configuration Mode

Defaults

- color-mode - blind
- interval - none
- next-meter - next-meter
- type - Simple token bucket

Example

```
Your Product(config-meter)# meter-type simpleTokenBucket color-mode aware
interval 10 cir 1000
```

Note: Meter should have been created.

Related Command(s)

- meter – Creates a Meter.
- show meter – Displays the Meter entry.

set policy

Command Objective This command sets CLASS for policy.

The no form of the command sets the default value for interface in this policy.

Syntax **set policy [class <integer(0-65535)>] [interface <iftype> <ifnum>] default-priority-type { none | { vlanPri | ipTos | ipDscp | mplsExp } <integer(0-63)> }**

no set policy interface

Parameter Description

- `class <integer(0-65535)` - Traffic CLASS for which the policy-map needs to be applied.
- `iftype` - Interface type
- `ifnum` - Interface number
- `default-priority-type<integer(0-63)>` - Per-Hop Behvior (PHB) type to be used for filling the default PHB for the policy-map entry. The types are:
  - `none`– No specific PHB type is set.
  - `vlanPri`– VLAN priority.
  - `ipTos`– IP Type of Service.
  - `ipDscp`– IP Differentiated Services Code Point.
  - `mplsExp`– MPLS Experimental

Mode Policy Map Configuration Mode

Defaults class - 0

Example

```
Your Product(config-ply-map)# set policy class 1 interface gigabitethernet
0/1 default-priority-type none
```

Note: CLASS should have been created.

Related Command(s)

- `class-map` – Adds a Class Map Entry.
- `policy-map` – Creates a policy map.
- `show policy-map` – Displays the Policy Map Entry.

set meter

Command Objective This command sets Policy parameters such as Meter and Meter Actions.

The no form of the command removes the Meter from the Policy and the Meter Actions.

Syntax **set meter <integer(1-65535)> [conform-action { drop | set- cos-transmit <short(0-7)>**

set-de-transmit <short(0-1)> | set-port <iftype> <ifnum> | set-inner-vlan-pri <short(0-7)> |set-mpls-exp-transmit <short(0-7)> | set-ip-prec-transmit <short(0-7)> | set-ip-dscp-transmit <short(0-63)> }] [exceed-action {drop | set-cos-transmit <short(0-7)> set-de-transmit <short(0-1)> | set-inner-vlan-pri <short(0-7)> | set-mpls-exp-transmit <short(0-7)> | set-ip-prec-transmit <short(0-7)> | set-ip-dscp-transmit <short(0-63)> }] [violate-action {drop | set-cos-transmit <short(0-7)> set- de-transmit <short(0-1)> | set-inner-vlan-pri <short(0-7)> | set-mpls-exp-transmit <short(0-7)> | set-ip-prec-transmit <short(0-7)> | set-ip-dscp-transmit <short(0-63)> }] [set-conform-newclass <integer(0-65535)>] [set-exceed-newclass <integer(0-65535)>] [set-violate-newclass <integer(0-65535)>]

no set meter

Parameter Description

- `<integer(1-65535)>` - Meter table identifier which is the index for the Meter table.
- `conform-action` - Action to be performed on the packet, when the packets are found to be In profile (conform). Options are:
    - `drop`– No action is configured.
    - `set-cos-transmit<short(0-7)>` – Sets the VLAN priority of the outgoing packet. This value ranges 0 and 7.
    - `set-de-transmit<short(0-1)>` – Sets the VLAN Drop Eligible indicator of the outgoing packet. This value ranges between 0 and 1.
    - `set-port<iftype> <ifnum>`– Sets the new port value.
    - `set-inner-vlan-pri<short(0-7)>` – Sets the inner VLAN priority of the outgoing packet. This value ranges between 0 and 7.
    - `set-mpls-exp-transmit<short(0-7)>` – Sets the MPLS Experimental bits of the outgoing packet. This value ranges between 0 and 7. It is not supported.
    - `set-ip-prec-transmit<short(0-7)>` – Sets the new IP TOS value. This value ranges between 0 and 7.
    - `set-ip-dscp-transmit<short(0-63)>` – Sets the new DSCP value. This value ranges between 0 and 63.
- `exceed-action` - Action to be performed on the packet, when the packets are found to be In profile (exceed). Options are:
    - `drop`– Drops the packet.
    - `set-cos-transmit<short(0-7)>` – Sets the VLAN priority of the outgoing packet. This value ranges 0 and 7.
    - `set-de-transmit<short(0-1)>` – Sets the VLAN Drop Eligible indicator of the outgoing packet. This value ranges between 0 and 1.

  - set-port<iftype> <ifnum>– Sets the new port value.
  - set-inner-vlan-pri<short(0-7)> – Sets the inner VLAN priority of the outgoing packet. This value ranges between 0 and 7.
  - set-mpls-exp-transmit<short(0-7)> – Sets the MPLS Experimental bits of the outgoing packet. This value ranges between 0 and 7. It is not supported.
  - set-ip-prec-transmit<short(0-7)> – Sets the new IP TOS value. This value ranges between 0 and 7.
  - set-ip-dscp-transmit<short(0-63)> – Sets the new DSCP value. This value ranges between 0 and 63.
- violate-action - Action to be performed on the packet, when the packets are found to be out of profile. Options are:
  - drop– Drops the packet.
  - set-cos-transmit<short(0-7)> – Sets the VLAN priority of the outgoing packet. This value ranges 0 and 7.
  - set-de-transmit<short(0-1)> – Sets the VLAN Drop Eligible indicator of the outgoing packet. This value ranges between 0 and 1.
  - set-port<iftype> <ifnum>– Sets the new port value.
  - set-inner-vlan-pri<short(0-7)> – Sets the inner VLAN priority of the outgoing packet. This value ranges between 0 and 7.
  - set-mpls-exp-transmit<short(0-7)> – Sets the MPLS Experimental bits of the outgoing packet. This value ranges between 0 and 7. It is not supported.
  - set-ip-prec-transmit<short(0-7)> – Sets the new IP TOS value. This value ranges between 0 and 7.
  - set-ip-dscp-transmit<short(0-63)> – Sets the new DSCP value. This value ranges between 0 and 63.
- set-conform-newclass<integer(0-65535)> - Represents the Traffic CLASS to which an incoming frame pattern is classified after metering. This value ranges between 0 and 65535.
- set-exceed-newclass<integer(0-65535)> - Represents the Traffic CLASS to which an incoming frame pattern is classified after metering. This value ranges between 0 and 65535.
- set-violate-newclass<integer(0-65535)> - Represents the Traffic CLASS to which an incoming frame pattern is classified after metering. This value ranges between 0 and 65535.

Mode Policy Map Configuration Mode

Defaults

- set-cos-transmit - 0
- set-de-transmit - 0

- set-mpls-exp-transmit - 0
- set-inner-vlan-pri - 0

Example

```
Your Product(config-ply-map)# set meter 1 conform-action drop exceed-action
drop violate-action drop set-conform- newclass 1 set-exceed-newclass 1 set-
violate-newclass 1
```

Note:VLAN priority can be set to a non-zero value only when MPLS Experimental bits is set to zero.

Related Command(s) `Show policy-map` - Displays the Policy Map entry

et algo-type

Command Objective This command sets Q Template entry parameters.

Syntax **set algo-type { tailDrop | headDrop | red | wred } [queue- limit <integer(1-65535)>] [queue-drop-algo {enable | disable }]**

Parameter Description

- `algo-type` - Type of drop algorithm used by the queue template. Options are:
  - `tailDrop` – Beyond the maximum depth of the queue, all newly arriving packets will be dropped. It is not supported in some models.
  - `headDrop` – Packets currently at the head of the queue are dropped to make room for the new packet to be enqueued at the tail of the queue, when the current depth of the queue is at the maximum depth of the queue. It is not supported in some models.
  - `red` – On packet arrival, an Active Queue Management algorithm is executed which may randomly drop a packet. It is not supported in some models.
  - `wred` – On packet arrival, an Active Queue Management algorithm is executed which may randomly drop a packet.
- `queue-limit<integer(1-65535)>` - Queue size. This value ranges between 1 and 65535.
- `queue-drop-algo` - Enable/disable Drop Algorithm for Congestion Management. Options are:
  - `enable`– Enables Drop Algorithm.
  - `disable` – Disables Drop Algorithm.

Mode Queue Template Configuration mode

Defaults

- queue-drop-algo - disable
- Drop-type - Taildrop
- Queue-limit - 10000

Example `Your Product(config-qtype)# set algo-type red queue-limit 18 queue-drop-algo enable`

Notes:

- Queue size must be greater than or equal to the minimum average threshold and less than or equal to the maximum average threshold.
- Drop algorithm for Congestion Management can be enabled only when the Random Detect Table entry is created for the Queue.

Related Command(s)

- `random-detect dp` – Sets Random Detect Table entry parameters.
- `show queue-template` – Displays the Q Template and Random Detect configurations.

random-detect dp

Command Objective This command sets Random Detect Table entry parameters.

The no form of the command deletes Random Detect Table entry.

Syntax **random-detect dp <short(0-2)> [min-threshold <short(1-65535)>] [max-threshold <short(1-65535)>] [max-pkt-size <short(1-65535)>] [mark-probability-denominator <short(1-100)>] [exponential-weight <integer(0-31)>]**

no random-detect dp <short(0-2)>

Parameter Description

- `dp<short(0-2)>` - Drop Precedence. Options are:
  - `0` **–** low drop precedence.
  - `1` **–** medium drop precedence.
  - `2` **–** high drop precedence.
- `min-threshold<short(1-65535)>` - Minimum average threshold for the random detect algorithm. This value ranges between 1 and 65535.
- `max-threshold<short(1-65535)>` - Maximum average threshold for the random detect algorithm. This value ranges between 1 and 65535.
- `max-pkt-size<short(1-65535)>` - Maximum allowed packet size. This value ranges between 1 and 65535.
- `mark-probability-denominator<short(1-100)>` - Maximum probability of discarding a packet in units of percentage. This value ranges between 1 and 100.
- `exponential-weight<integer(0-31)>` - Exponential weight for determining the average queue size. This value ranges between 0 and 31.

Mode Queue Template Configuration Mode

Defaults

- mark-probability-denominator - 100
- exponential-weight - 0

Example

```
Your Product(config-qtype)# random-detect dp 1 min- threshold 1200 max-
threshold 13000 max-pkt-size 100 mark- probability-denominator 50
exponential-weight 30
```

show qos global info

Command Objective This command displays QoS related global configurations.

Syntax **show qos global info**

Mode Privileged EXEC Mode

Example

```
Your Product# show qos global info
QoS Global Information
-----------------------------------
System Control              : Start
System Control              : Enable
Rate Unit                   : kbps
Rate Granularity            : 64
Trace Flag                  : 0
```

Related Command(s)

- `shutdown qos` – Shutsdown the QoS subsystem.
- `qos` – Enables or disables the QoS subsystem.

show priority-map

Command Objective This command displays the Priority Map entry.

Syntax **show priority-map [<priority-map-id(1-65535)>]**

Parameter Description `<priority-map-id(1-65535)>` - Output priority map index for the incoming packet received over ingress Port/VLAN with specified incoming priority.

Mode Privileged EXEC Mode.

Example

```
Your Product# show priority-map
QoS Priority Map Entries
========================
PriorityMapId               : 1
```

```
IfIndex                     : 1
VlanId                      : 4094
InPriorityType              : VlanPriority
InPriority                  : 0
RegenPriority               : 7
InnerRegenPriority          : 1
PriorityMapId               : 9
IfIndex                     : gi 0/5
VlanId                      : 2
InPriorityType              : IP Protocol
InPriority                  : 1
RegenPriority               : 5
InnerRegenPriority          : 7
```

Note: If executed without the optional parameters, this command displays all the available Priority Map information.

Related Command(s)

- `priority-map` – Adds a Priority Map entry
- `map` - Adds a Priority Map entry for mapping an incoming priority to a regenerated priority

show class-map

Command Objective This command displays the Class Map entry.

Syntax **show class-map [<class-map-id(1-65535)>]**

Parameter Description `<class-map-id(1-65535)>` - Index that enumerates the MultiField Classifier table entries.

Mode Privileged EXEC Mode.

Example

```
Your Product# show class-map
QoS Class Map Entries
=====================
ClassMapId                  : 1
L2FilterId                  : None
L3FilterId                  : None
PriorityMapId               : 1
CLASS                       : 1000
PolicyMapId                 : 1
PreColor                    : None
Status                      : Active
```

Note: If executed without the optional parameters, this command displays all the available Class Map information

Related Command(s)

- `class-map` – Adds a Class Map entry.
- `priority-map` – Adds a Priority Map entry

show class-to-priority-map

Command Objective This command displays the class group entry.

Syntax **show class-to-priority-map <group-name(31)>**

Parameter Description `<group-name(31)>`- Unique identification of the group to which an input CLASS belongs.

Mode Privileged EXEC Mode.

Example

```
Your Product# show class-to-priority-map CLASS1
QoS Class To Priority Map Entries
---------------------------------
GroupName         : CLASS1
Class               LocalPriority
----------------------------------
2                        2
```

Related Command(s)

- `show class-map` – Displays the Class Map entry.
- `set class` – Sets CLASS for L2and/or L3 filters or Priority Map ID and adds a CLASS to Priority Map Entry with regenerated priority.

show meter

Command Objective This command displays the Meter entry.

Syntax **show meter [<meter-id(1-65535)>]**

Parameter Description `<meter-id(1-65535)>` - Index that enumerates the Meter entries. This value ranges between 1 and 65535.

Mode Privileged EXEC Mode.

Example

```
Your Product# show meter
QoS Meter Entries
=================
MeterId                     : 1
Type                        : Simple Token Bucket
Color Mode                  : Color Aware
```

```
Interval                    : 10
CIR                         : 1000
CBS                         : None
EIR                         : None
EBS                         : None
NextMeter                   : None
Status                      : Active
```

Note: If executed without the optional parameters, this command displays all the available Meter information.

Related Command(s) `set meter` – Sets Policy parameters such as Meter and Meter Actions.

show policy-map

Command Objective This command displays the Policy Map entry.

Syntax **show policy-map [<meter-id(1-65535)>]**

Parameter Description `<meter-id(1-65535)>` - Index that enumerates the Meter entries.

Mode Privileged EXEC Mode.

Example

```
Your Product# show policy-map
QoS Policy Map Entries
====================== PolicyMapId      : 1
IfIndex      : 0
Class        : 0
DefaultPHB   : None. MeterId      : 1
ConNClass    : 0
ExcNClass    : 0
VioNClass    : 0
ConfAct      : Port 1
ExcAct       : Drop.
VioAct       : Drop.
```

Note: If executed without the optional parameter, this command displays all the available Policy Map. information

Related Command(s) `set policy` – Sets CLASS for policy.

show queue-template

Command Objective This command displays the Q Template and Random Detect configurations.

Syntax **show queue-template [<queue-template-Id(1-65535)>]**

Parameter Description `<queue-template-Id(1-65535)>-Id` - Queue Template Table index.

Mode Privileged EXEC Mode.

Example

```
Your Product# show queue-template
Queue Template Entries
------------------------------------
Q Template Id                : 1
Q Limit                      : 10000
Drop Type                    : Tail Drop
Drop Algo Status             : Disable
If executed without the optional parameter, this command displays all the available
Queue Template information.
```

Related Command(s) `queue-type` – Creates a Queue Template Type.

show shape-template

Command Objective This command displays the Shape Template configurations.

Syntax show shape-template [<shape-template-Id(1-65535)>]

Parameter Description `<shape-template-Id(1-65535)>` - Shape Template Table index.

Mode Privileged EXEC Mode.

Example

```
Your Product# show shape-template
QoS Shape Template Entries
------------------------------------------------------------------
ShapeTemplate Id        CIR       CBS     EIR     EBS
----------------        ---       ---     ---     ---
1                       1         1       1       1
```

Note: If executed without the optional parameter, this command displays all the available Shape Template information

Related Command(s) `shape-template` – Creates a Shape Template.

show scheduler

Command Objective This command displays the configured Scheduler.

Syntax **show scheduler [interface <iftype> <ifnum>]**

Parameter Description

- `iftype` - Interface type.
- `ifnum` - Interface number.

Mode Privileged EXEC Mode.

Example

```
Your Product# show scheduler
QoS Scheduler Entries
---------------------------------
IfIndex Scheduler Index Scheduler Algo Shape Index
Scheduler HL GlobalId
----------- ----------------------- ---------------------- ------------------ -------------
------- -------------
Gi0/1    1              strictPriority    0           0
1
```

Note: If executed without the optional parameter, this command displays all the available scheduler entries.

Related Command(s) `scheduler` – Creates a Scheduler and configures the Scheduler parameters.

show queue

Command Objective This command displays the configured Queues.

Syntax **show queue [interface <iftype> <ifnum>]**

Parameter Description

- `iftype` - Interface type.
- `ifnum` - Interface number.

Mode Privileged EXEC Mode.

Example

```
Your Product# show queue
QoS Queue Entries
---------------------------
IfIndex Queue Idx Queue Type Scheduler Idx Weight Priority
Shape Idx Global Id
----------- -------------- ---------------- -------------------- ---------- -------------
-------------------------------------
Gi0/1     1         1          1          1       1
1        1
```

Note: If executed without the optional parameter, this command displays all the available queue entries

Related Command(s)

- `queue` – Creates a Queue and configures the Queue parameters.
- `queue-type` – Creates a Queue Template Type.
- `show queue-template` – Displays the Q Template and Random Detect configurations.

show queue-map

Command Objective This command displays the configured Queue map.

Syntax **show queue-map [interface <iftype> <ifnum>]**

Parameter Description

- `iftype` - Interface type.
- `ifnum` - Interface number.

Mode Privileged EXEC Mode.

Example

```
Your Product# show queue-map
QoS Queue Map Entries
---------------------------------
IfIndex                  CLASS    PriorityType  Priority Value      Mapped
Queue
-----------
-                        --------  -------------------  ----------------------      -------------
Gi0/1                    1  none   0      1
```

Note: If executed without the optional parameter, this command displays all the available queue map entries.

Related Command(s) `queue-map` – Creates a Map for a Queue with Class or regenerated priority.

show sched-hierarchy

Command Objective This command displays the configured hierarchy scheduler.

Syntax **show sched-hierarchy [interface <iftype> <ifnum>]**

Parameter Description

- `iftype` - Interface type.
- `ifnum` - Interface number.

Mode Privileged EXEC Mode.

Example

```
Your Product# show sched-hierarchy
QoS Hierarchy Scheduler Entries
------------------------------------------------
IfIndex Hierarchy Level
Id Weight Priority       Sched Index     NextQueue Id  NextSched
----------- ------------------------  -----------------     -------------------  ----------------
---- ---------- -------------
```

```
Gi0/1         1
1       1                  1  0       2
```

Note: If executed without the optional parameter, this command displays all the available hierarchy scheduler entries

Related Command(s)

- `scheduler` – Creates a Scheduler and configures the Scheduler parameters.
- `sched-hierarchy` – Creates a Scheduler Hierarchy.

show qos pbit-preference-over-Dscp

Command Objective This command displays configured pbit reference for the tagged ports.

Syntax **show qos pbit-preference-over-Dscp [interface <iftype> <ifnum>]**

Parameter Description

- `iftype` - Interface type.
- `ifnum` - Interface number.

Mode Privileged EXEC Mode.

Example

```
Your Product# show qos pbit-preference-over-Dscp
QoS Default Pbit Preference Entries
--------------------------------- IfIndex Pbit preference over DSCP
------------- ---------------------------------------- Gi0/1    Enabled
```

Note: If executed without the optional parameter, this command displays all the available scheduler entries

Related Command(s)

- `scheduler` – Creates a Scheduler and configures the Scheduler parameters.
- `sched-hierarchy` – Creates a Scheduler Hierarchy.

show qos def-user-priority

Command Objective This command displays the configured default ingress user priority for a port.

Syntax **show qos def-user-priority [interface <iftype> <ifnum>]**

Parameter Description

- `iftype` - Interface type.
- `ifnum` - Interface number.

Mode Privileged EXEC Mode.

Example

```
Your Product# show qos def-user-priority
QoS Default User Priority Entries
-------------------------------- IfIndex     Default User Priority
------------ --------------------------------
Gi0/1           0
Gi0/2           0
Gi0/3           0
Gi0/4           0
Gi0/5           0
Gi0/6           0
Gi0/7           0
Gi0/8           0
Gi0/9           0
Gi0/10          0
Gi0/11          0
Gi0/12          0
Gi0/13          0
Gi0/14          0
Gi0/15          0
Gi0/16          0
Gi0/17          0
Gi0/18          0
Gi0/19          0
Gi0/20          0
Gi0/21          0
Gi0/22          0
Gi0/23          0
Gi0/24          0
```

Note: If executed without the optional parameter, this command displays the available default ingress user priority entries for all the interface.

Related Command(s) `qos interface` – Sets the default ingress user priority for the port.

show qos meter-stats

Command Objective This command displays the Meters statistics for conform, exceed, violate packets and octets count.

Syntax **show qos meter-stats [<Meter-Id(1-65535)>]**

Parameter Description `<Meter-Id(1-65535)>` - Index that enumerates the Meter entries.

Mode Privileged EXEC Mode.

Example

```
Your Product# show qos meter-stats
```

```
QoS Meter (Policer) Stats
------------------------------------------------------------
Meter Index                   : 1
Conform Packets               : 00
Conform Octects               : 00
Exceed Packets                : 00
Exceed Octects                : 00
Violate Packets               : 00
Violate Octects               : 0
```

Note: If executed without the optional parameter, this command displays the Meter statistics for all the available Meters.

Related Command(s)

- `show meter` – Displays the Meter entry.
- `set meter` – Sets Policy parameters such as Meter and Meter Actions.

show qos queue-stats

Command Objective This command displays Queue statistics for EnQ, DeQ, discarded packets and octets Count, Management Algo Drop and Q occupancy.

Syntax **show qos queue-stats [interface <iftype> <ifnum>]**

Parameter Description

- `iftype` - Interface Type.
- `ifnum` - Interface Number.

Mode Privileged EXEC Mode.

Example

```
Your Product# show qos queue-stats
QoS Queue Stats
------------------------------------------------------------
Interface Index               : Gi 0/1
Queue Index                   : 2
EnQ Packets                   : 00
EnQ Octects                   : 00
DeQ Packets                   : 00
DeQ Octects                   : 00
Discard Packets               : 00
Discard Octects               : 00
Occupancy Octects             : 00
CongMgntAlgoDrop Octects      : 00
```

Note: If executed without the optional parameter, this command displays the Queue statistics for all the available Interfaces.

Related Command(s) `show queue` – Displays the configured Queues.

debug qos

Command Objective This command sets the debug level for QOS module.

The no form of the command resets the debug level for QoS module.

Syntax **debug qos {initshut | mgmt | ctrl | dump | os | failall | buffer}**

no debug qos {initshut | mgmt | ctrl | dump | os | failall | buffer}

Parameter Description

- `initshut` - Generates debug statements for Init and shutdown traces
- `mgmt` - Generates debug statements for Management traces
- `ctrl` - Generates debug statements for Control plane traces
- `dump` - Generates debug statements for Packet dump traces
- `os` - Generates debug statements for Traces related to all resources except buffers
- `failall` - Generates debug statements for All failure traces
- `buffer` - Generates debug statements for Buffer allocation / release traces

Mode Privileged EXEC Mode

Example

```
Your Product# debug qos initshut
```

qos pbit-preference

Command Objective This command sets qbit preference value. Setting this to enable indicates that if a frame includes both 802.1p and a DSCP field, then the pbit field takes precedence. For DSCP to take precedence, set to Disable.

Syntax **qos pbit-preference {enable | disable}**

Parameter Description

- `enable` - Enables the feature
- `disable` - Disables the feature

Mode Interface Configuration mode

Default Disabled

Example

```
Your Product(config-if)# qos pbit-preference enable
```

cpu rate limit queue

Command Objective This command is used to configure rates for a CPU port Queues.

Syntax **cpu rate limit queue <integer(1-65535)> minrate <integer(1-65535)> maxrate <integer(1-65535)>**

Parameter Description

- `<integer(1-65535)>` - Queue Identifier that uniquely identifies the queue in the system/port. This value ranges between 1 and 65535.
- `minrate <integer(1-65535)>` - minimum transmission rate on a cpu port. This value ranges between 1 and 65535. Minimum Rate must be less than or equal to Max Rate.
- `maxrate <integer(1-65535)>` - maximum transmission rate on a cpu port. This value ranges between 1 and 65535. Max Rate must be greater than or equal to Min Rate.

Mode Global Configuration Mode

Defaults Enabled

Example `Your Product(config)# cpu rate limit queue 1 minrate 10 maxrate 100`

Related Command(s) `Show cpu rate limit` – Display the rate limiting values for CPU.

show cpu rate limit

Command Objective This command is used to display the rate limiting values for CPU.

Syntax **show cpu rate limit**

Parameter Description

- `iftype` - Interface type.
- `ifnum` - Interface number.

Mode Privileged EXEC Mode.

Example

```
Your Product# show cpu rate limit
QoS CPU Queue Rate Limit Table
---------------------------------------------------------------
Queue ID                 MinRate  MaxRate
-------                  -------  -------
1                        1        65535
2                        1        65535
3                        1        65535
4                        1        65535
5                        1        65535
6                        1        65535
7                        1        65535
8                        1        65535
```

Related Command(s) `cpu rate limit queue` – Configure rates for a CPU port Queues

28 ACL

ACLs (Access Control Lists) filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. ACLs are used to block IP/MAC packets from being forwarded by a switch. The switch examines each packet to determine whether to forward or drop the packet, based on the criteria specified within the access lists.

Access list criteria can be the source address of the traffic, the destination address of the traffic, the upper- layer protocol or other information.

There are many reasons to configure access lists - access lists can be used to restrict contents of routing updates or to provide traffic flow control. But one of the most important reasons to configure access lists is to provide security for the network.

Access lists must be used to provide a basic level of security for accessing the network. If access lists has not been configured on the router, all packets passing through the router can be allowed onto all parts of the network.

For example, access lists can allow one host to access a part of the network and prevent another host from accessing the same area.

The list of CLI commands for the configuration of ACL is as follows:

- ip access-list
- mac access-list extended
- permit - standard mode
- deny - standard mode
- copy-to-cpu - standard mode
- permit- ip/ospf/pim/protocol type
- permit ipv6
- deny - ip/ospf/pim/protocol type
- deny ipv6
- copy-to-cpu - ip / ospf / pim / protocol-type
- copy-to-cpu ipv6
- permit tcp
- deny tcp
- copy-to-cpu tcp
- permit udp
- deny udp
- copy-to-cpu udp
- permit icmp
- deny icmp

- copy-to-cpu icmp
- permit icmpv6
- deny icmpv6
- copy-to-cpu icmpv6
- ip access-group
- mac access-group
- permit - MAC
- deny - MAC
- copy-to-cpu - MAC
- show access-lists
- storm-control
- rate-limit-output

ip access-list

Command Objective This command creates IP ACLs and enters the IP Access-list configuration mode. Standard access lists create filters based on IP address and network mask only (L3 filters only). Extended access lists enables the specification of filters based on the type of protocol, range of TCP/UDP ports as well as the IP address and network mask (Layer 4 filters).

Depending on the standard or extended option chosen by the user, this command returns a corresponding IP Access list configuration mode.

The no form of the command deletes the IP access-list.

Syntax **ip access-list {standard <access-list-number (1-1000)> | extended <access-list-number (1001-65535)> }**

no ip access-list {standard <access-list-number (1-1000)> | extended <access-list-number (1001-65535)>}

Parameter Description

- `standard <access-list-number (1-1000)>` - Configures the standard access-list number. this value ranges between 1 and 1000
- `extended <access-list-number (1001-65535)>` - Configures the extended access-list number. This value ranges between 1001 and 65535.

Mode Global Configuration Mode

Note: ACLs on the system perform both access control and Layer 3 field classification. To define Layer 3 fields' access-lists the ip access-list command must be used.

Example

```
Your Product (config)# ip access-list standard 1
```

Related Command(s)

- permit - standard mode - Specifies the packets to be forwarded depending upon the associated parameters
- deny - standard mode - Denies traffic if the conditions defined in the deny statement are matched
- copy-to-cpu - standard mode - Copies the IP control packets to control plane CPU with or without switching of packets based on the configured parameters.
- permit- ip/ospf/pim/protocol type - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- permit ipv6 - Specifies IP packets to be forwarded based on protocol and associated parameters.
- deny - ip/ospf/pim/protocol type- Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched
- copy-to-cpu - ip / ospf / pim / protocol-type - Copies the IP control packets of all type of protocols to control plane CPU with or without switching of packets based on the configured parameters.
- deny ipv6 - Specifies IPv6 packets to be rejected based on protocol and associated parameters.
- copy-to-cpu ipv6 - Copies the IPv6 control packets to control plane CPU with or without switching of packets based on the configured parameters.
- permit tcp - Specifies the TCP packets to be forwarded based on the associated parameters
- deny tcp - Specifies the TCP packets to be rejected based on the associated parameters
- copy-to-cpu tcp - Copies the TCP control packets to control plane CPU with or without switching of packets based on the configured parameters.
- permit udp - Specifies the UDP packets to be forwarded based on the associated parameters
- deny udp - Specifies the UDP packets to be rejected based on the associated parameters
- copy-to-cpu udp - Copies the UDP control packets to control plane CPU with or without switching of packets based on the configured parameters.
- permit icmp - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters
- deny icmp - Specifies the ICMP packets to be rejected based on the IP address and associated parameters
- copy-to-cpu icmp - Copies the ICMP control packets to control plane CPU with or without switching of packets based on the configured parameters.
- ip access-group - Enables access control for the packets on the interface
- show access-lists - Displays the access list configuration

mac access-list extended

Command Objective This command creates Layer 2 MAC ACLs, that is, this command creates a MAC access-list and returns the MAC-Access list configuration mode to the user. This value ranges between 1 and 65535.

The no form of the command deletes the MAC access-list.

Syntax **mac access-list extended <access-list-number (1-65535)>**

no mac access-list extended <short (1-65535)>

Mode Global Configuration Mode

Note: ACLs on the system perform both access control and layer 2 field classification. To define Layer 2 access lists, the mac access-list command must be used.

Example Your Product (config)# mac access-list extended 5

Related Command(s)

- `mac access-group` - Applies a MAC access control list (ACL) to a Layer 2 interface.
- `permit – MAC` - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- `deny – MAC` - Specifies the packets to be rejected based on the MAC address and the associated parameters
- `copy-to-cpu – MAC` - Copies the MAC protocol control packets to control plane CPU with or without switching of packets based on the configured parameters.
- `show access-lists` - Displays the access lists configuration.

permit - standard mode

Command Objective This command specifies the packets to be forwarded depending upon the associated parameters. Standard IP access lists use source addresses for matching operations.

Syntax **permit { any | host <src-ip-address> | <src-ip-address> <mask> } [{ any | host <dest-ip-address> | <dest-ip- address> <mask> }]**

Parameter Description

- any|host <src-ip-address>| < src-ip-address><mask> -Source IP address can be
    - 'any' or
    - the word 'host' and the dotted decimal address or
    - the IP address of the host that the packet is from and the network mask to use with thesource IP address
- any|host <dest-ip-address>| < dest-ip-address ><mask> - Destination IP address can be
    - 'any' or
    - the word 'host' and the dotted decimal address or
    - the Ip address of the host that the packet is destined for and the network mask to use with the destination IP address

Mode IP ACL Configuration (standard)

Example Your Product(config-std-nacl)# permit host 100.0.0.10 host 10.0.0.1

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `deny` - standard mode - Denies traffic if the conditions defined in the deny statement are matched
- `show access-lists` - Displays the access list configuration

deny - standard mode

Command Objective This command denies traffic if the conditions defined in the deny statement are matched.

Syntax **deny{ any | host <src-ip-address> | <src-ip-address> <mask>} [{ any | host <dest-ip-address> | <dest-ip-address> <mask> }]**

Parameter Description

- any|host src-ip-address | <src-ip-address> <mask> - Source IP address can be
  - 'any' or
  - the word 'host' and the dotted decimal address or
  - The network number of the host that the packet is from and the network mask to use with the source IP address
- any|host dest-ip-address| <dest-ip-address><mask> - Destination IP address can be
  - 'any' or
  - the word 'host' and the dotted decimal address or
  - the network number of the host that the packet is destined for and the network mask to use with the destination IP address

Mode IP ACL Configuration (standard)

Example

```
Your Product(config-std-nacl)# deny host 100.0.0.10 any
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `permit - standard mode` - Specifies the packets to be forwarded depending upon the associated parameters
- `show access-lists` - Displays the access list configuration

copy-to-cpu - standard mode

Command Objective This command copies the IP control packets to control plane CPU with or without switching of packets based on the configured parameters.

Syntax **copy-to-cpu { any | host <src-ip-address> | <src-ip- address> <mask> } [{ any | host <dest-ip-address> | <dest-ip-address> <mask> }] [noswitching]**

Parameter Description

- `any | host <src-ip-address> | <src-ip-address> <mask>` - Copies the IP control packets to control plane CPU with or without switching of packets based on the following source address configuration:

  - `any` - Copies all control packets. Does not check for the source IP address in the packets.
  - `host` - Copies only the control packets having the specified unicast host network IP address as the source address.
  - `<src-ip-address> <mask>` - Copies only the control packets having the specified unicast source IP address and mask.

- `any | host <dest-ip-address> | <dest-ip-address> <mask>`
  - Copies the IP control packets to control plane CPU with or without switching of packets based on the following destination address configuration:
    - `any` - Copies all control packets. Does not check for the destination IP address in the packets.
    - `host` - Copies only the control packets having the specified host network IP address as the destination address.
    - `<dest-ip-address> <mask>` - Copies only the control packets having the specified destination IP address and mask.
- `noswitching` - Copies the IP control packets to control plane CPU without switching of packets.

  Note: This parameter is not supported in some models due to hardware limitation.

Mode ACL Standard Access List Configuration Mode

Defaults

- any | host <src-ip-address> | <src-ip-address> <mask> - any
- any | host <dest-ip-address> | <dest-ip-address> <mask> - any

Example

```
Your Product (config-std-nacl)# copy-to-cpu host 30.0.0.4 any noswitching
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `show access-lists` - Displays the access lists configuration.

permit- ip/ospf/pim/protocol type

Command Objective This command allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched.

Syntax **permit { ip | ospf | pim | <protocol-type (1-255)>}{ any | host <src-ip-address> | <src-ip-address> <mask> }{ any | host <dest-ip-address> | <dest-ip-address> <mask> }[{tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp {<value (0-63)>}] [priority <value (1-255)>]**

Parameter Description

- `ip| ospf|pim|<protocol-type (1-255)>` - Type of protocol for the packet. It can also be a protocol number.
- `any| host <src-ip-address>|<src-ip-address> <mask>` - Source IP address can be
    - 'any' or
    - the dotted decimal address or
    - the IP Address of the network or the host that the packet is from and the network mask to use with the source address.
- `any|host <dest-ip-address>|<dest-ip-address> <mask>` - Destination IP address can be
    - 'any' or
    - the dotted decimal address or
    - the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address
- `tos` - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7.
- `dscp` - Differentiated services code point provides the quality of service control. The various options available are:
    - `0-63` - Differentiated services code point value
- `priority` - The priority of the L3 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
    - This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults none

Note: Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.

Example

```
Your Product (config-ext-nacl)# permit 200 host 100.0.0.10 any tos 6 load
balance src-ip
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `deny - ip/ospf/pim/protocol type` - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched
- `show access-lists` - Displays the access list configuration

permit ipv6

Command Objective This command specifies IP packets to be forwarded based on protocol and associated parameters.

Syntax **permit ipv6 { flow-label <integer(1-65535)> | {any | host <ip6_addr> <integer(0-128)> } {**

any | host <ip6_addr> <integer(0-128)> }}

Parameter Description

- `flow-label` - Flow identifier in IPv6 header.
- `any | host <ip6_addr> <integer(0-128)>` - Source address of the host / any host.
- `any | host <ip6_addr> <integer(0-128)>` - Destination address of the host / any host.

  Note: This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults priority - 1

Note: Flow label cannot be configured along with either source/destination IP address.

Example

```
Your Product (config-ext-nacl)# permit ipv6 host c004::04
28 any load-balance src-ip
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `show access-lists` - Displays the access lists configuration.

deny - ip/ospf/pim/protocol type

Command Objective This command denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched.

Syntax **deny { ip | ospf | pim | <protocol-type (1-255)>} { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> } [{tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp {<value (0-63)> }] [priority<value (1-255)>]**

Parameter Description

- `ip| ospf|pim|<protocol-type (1-255)>` - Type of protocol for the packet. It can also be a protocol number.
- `any| host <src-ip-address>|<src-ip-address> <mask>` - Source IP address can be
  - **'**any**'** or
  - the word **'**host**'** and the dotted decimal address or
  - number of the network or the host that the packet is from and the network mask to use with the source address
- `any|host <dest-ip-address>|<dest-ip-address> <mask>` - Destination IP address can be

    - ‘any’ or
    - the word ‘host’ and the dotted decimal address or
    - number of the network or the host that the packet is destined for and the network mask to use with the destination address
- `tos` - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7.
- `dscp` - Differentiated services code point provides the quality of service control. The various options available are:
    - 0-63 - Differentiated services code point value
- `priority` - The priority of the L3 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of ‘filter priority’ implies a higher priority.
    - This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults None

Notes:

- Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.
- Service Vlan, Service Vlan Priority, Customer Vlan and Customer Vlan Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.

Example

```
Your Product (config-ext-nacl)# deny ospf any host
10.0.0.1 tos max-throughput
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `permit- ip/ospf/pim/protocol type` - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- `show access-lists` - Displays the access list configuration

deny ipv6

Command Objective This command specifies IPv6 packets to be rejected based on protocol and associated parameters.

Syntax **deny ipv6 { flow-label <integer(1-65535)> | {any | host <ip6_addr> <integer(0-128)> } { any | host <ip6_addr> <integer(0-128)> }}**

Parameter Description

- `flow-label` - Flow identifier in IPv6 header.
- `any | host <ip6_addr> <integer(0-128)>` - Source address of the host / any host.
- `any | host <ip6_addr> <integer(0-128)>` - Destination address of the host / any host.

  Note: This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults priority - 1

Note: Flow label cannot be configured along with either source/destination IP address.

Example

```
Your Product (config-ext-nacl)# deny ipv6 host c004::04 28 any
Your Product (config-ext-nacl)# deny ipv6 flow-label 40
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `show access-lists` - Displays the access lists configuration.

copy-to-cpu - ip / ospf / pim / protocol-type

Command Objective This command copies the IP control packets of all type of protocols to control plane CPU with or without switching of packets based on the configured parameters.

Syntax **copy-to-cpu { ip | ospf | pim | <protocol-type (1-255)>} { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> } [{tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>}] [priority <value (1-255)>] [noswitching]**

Parameter Description

- `ip | ospf | pim | <protocol-type (1-255)>` - Copies the IP control packets to control plane CPU with or without switching of packets based on the following protocol type configuration:
  - `ip` - Copies only the control packets of IP protocol.
  - `ospf` - Copies only the control packets of OSPF protocol.
  - `pim` - Copies only the control packets of PIM protocol.
  - `<protocol-type (1-255)>` - Copies only the control packets of administrator specified protocol type. This value ranges between 1 and 255.
- `any | host <src-ip-address> | <src-ip-address> <mask>` - Copies the IP control packets to control plane CPU with or without switching of packets based on the following source address configuration:
  - `any` - Copies all control packets. Does not check for the source IP address in the packets.

    - `host` - Copies only the control packets having the specified unicast host network IP address as the source address.
    - `<src-ip-address> <mask>` - Copies only the control packets having the specified unicast source IP address and mask.
- `any | host <dest-ip-addresq> | <dest-ip-address> <mask>` - Copies the IP control packets to control plane CPU with or without switching of packets based on the following destination address configuration:
    - `any` - Copies all control packets. Does not check for the destination IP address in the packets.
    - `host` - Copies only the control packets having the specified host IP address as the destination address.
    - `<dest-ip-address> <mask>` - Copies only the control packets having the specified destination IP address and mask.
- `tos` - Copies the IP control packets to control plane CPU with or without switching of packets based on the following type of service configuration:
    - max-reliability - Copies only the control packets having TOS field set as high reliability.
    - max-throughput - Copies only the control packets having TOS field set as high throughput.
    - min-delay - Copies only the control packets having TOS field set as low delay.
    - normal - Copies all control packets. Does not check for the TOS field in the packets.
    - <value (0-7)> - Copies the control packets based on the TOS value set. The value ranges between 0 and 7. This value represents different combination of TOS.
    - 0 - Copies all control packets. Does not check for the TOS field in the packets.
    - 1 - Copies only the control packets having TOS field set as high reliability.
    - 2 - Copies only the control packets having TOS field set as high throughput.
    - 3 - Copies the control packets having TOS field set either as high reliability or high throughput.
    - 4 - Copies only the control packets having TOS field set as low delay.
    - 5 - Copies the control packets having TOS field set either as low delay or high reliability.
    - 6 - Copies the control packets having TOS field set either as low delay or high throughput.
    - 7 - Copies the control packets having TOS field set either as low delay or high reliability or high throughput.
- `dscp` - Copies only the control packets having the specified DSCP value. This value ranges between 0 and 63.
- `priority` - Copies only the control packets having the specified L2 priority value. This value ranges between 1 and 255.
- `noswitching` - Copies the IP control packets to control plane CPU without switching of packets.

  Note: This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults

- ip | ospf | pim | <protocol-type (1-255)> - Control packets of all type of protocols are copied.

- any | host <src-ip-address> | <src-ip-address> <mask> - any
- any | host <dest-ip-addresq> | <dest-ip-address> <mask> - any
- dscp - -1 (that is, the packets are not checked for DSCP value)
- priority - 1

Example

```
Your Product (config-ext-nacl)# copy-to-cpu ospf host
30.0.0.4 any tos min-delay priority 2
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `show access-lists` - Displays the access lists configuration.

copy-to-cpu ipv6

Command Objective This command copies the IPv6 control packets to control plane CPU with or without switching of packets based on the configured parameters.

Syntax **copy-to-cpu ipv6 { flow-label <integer(1-65535)> | {any | host <ip6_addr> <integer(0-128)> } { any | host <ip6_addr> <integer(0-128)> }} [noswitching]**

Parameter Description

- `flow-label` - Copies only the IPv6 control packets having the specified flow identifier. This value ranges between 1 and 65535.
- `any | host <ip6_addr> <integer(0-128)>` - Copies the IPv6 control packets to control plane CPU with or without switching of packets based on the following source address configuration:
  - `any` - Copies all control packets. Does not check for the source IPv6 address in the packets.
  - `host` - Copies only the control packets having the specified source IPv6 address and prefix length.
- `any | host <ip6_addr> <integer(0-128)>` - Copies the IPv6 control packets to control plane CPU with or without switching of packets based on the following destination address configuration:
  - `any` - Copies all control packets. Does not check for the destination IPv6 address in the packets.
  - `host` - Copies only the control packets having the specified destination IPv6 address and prefix length.
- `noswitching` - Copies the IPv6 control packets to control plane CPU without switching of packets.

Note: This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults

- flow-label - 0 (that is, the packets are not checked for flow identifier)
- any | host <ip6_addr> <integer(0-128)> - any

Example Your Product (config-ext-nacl)# copy-to-cpu ipv6 flow-label 40

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `show access-lists` - Displays the access lists configuration.

permit tcp

Command Objective This command specifies the TCP packets to be forwarded based on the associated parameters.

Syntax **permit tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> }[{gt <port-number (1-65535)> | lt <port-number (1-65535)>|eq <port-number (1-65535)> |range <port-number (1-65535)> <port-number (1-65535)>}]{ any | host <dest-ip- address> | <dest-ip-address> <dest-mask> }[{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> |range <port-number (1-65535)> <port-number (1-65535)>}][{ ack | rst }][{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}|dscp {<value(0-63)>}] [priority <value(1-255)>]**

Parameter Description

- `tcp` - Transport Control Protocol
- `any| host <src-ip-address>|<src-ip-address> < src-mask >`
  - Source IP address can be
    - 'any' or
    - the dotted decimal address OR
    - the IP address of the network or the host that the packet is from and the network mask to use with the source address
- `port-number` - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.
  - eq=equal
  - lt=less than
  - gt=greater than
  - range=a range of ports; two different port numbers must be specified
- `any|host<dest-ip-address> |<dest-ip-address> < dest-mask`
  - Destination IP address can be
    - 'any' or
    - the dotted decimal address or
    - the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address
- `ack` - TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any

(3).

- `rst` - TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3).
- `tos` - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7.
- `dscp` - Differentiated services code point provides the quality of service control. The various options available are:
    - `0-63` - Differentiated services code point value
- `priority` - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

  Note: This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults

- tos-value - 0
- ack - 'any' (3) [indicates that the TCP ACK bit will not be checked to decide the action]
- rst - any' (3) [indicates that the TCP RST bit will not be checked to decide the action]
- dscp - -1
- priority - 1

Example

```
Your Product (config-ext-nacl)# permit tcp any 10.0.0.1 load-balance scr-ip
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `deny tcp` - Specifies the TCP packets to be rejected based on the associated parameters
- `show access-lists` - Displays the access list configuration

deny tcp

Command Objective This command specifies the TCP packets to be rejected based on the associated parameters.

Syntax **deny tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> }[{gt <port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}]{ any | host<dest-ip-address> | <dest-ip-address> <dest-mask> }[{gt<port-number (1-65535)> | lt <port-number (1-65535)> | eq<port-number (1-65535)> |range <port-number (1-65535)> <port-number (1-65535)>}][{ ack | rst }][{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp {<value (0-63)>}] [priority <value (1-255)>]**

Parameter Description

- `tcp` - Transmission control protocol

- `any| host <src-ip-address>|<src-ip-address> <src-mask>` - Source IP address can be
  - ‘any’ or
  - the word ‘host’ and the dotted decimal address or
  - number of the network or the host that the packet is from and the network mask to use with the source address
- `port-number` - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.
  - eq=equal
  - lt=less than
  - gt=greater than
  - range=a range of ports; two different port numbers must be specified
- `any|host <dest-ip-address>|<dest-ip-address> <dest- mask>` - Destination IP address can be
  - ‘any’ or
  - the word ‘host’ and the dotted decimal address or
  - number of the network or the host that the packet is destined for and the network mask to use with the destination address
- `ack` - TCP ACK bit to be checked against the packet. It can be establish (1), non-establish (2) or any (3)
- `rst` - TCP RST bit to be checked against the packet. It can be set (1), notset (2) or any (3)
- `tos` - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7.
- `dscp` - Differentiated services code point provides the quality of service control. The various options available are:
  - `0-63` - Differentiated services code point value
- `priority` - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of ‘filter priority’ implies a higher priority.

  Note: This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults

- tos-value - 0
- ack - ‘any’ (3) [indicates that TCP ACK bit will not be checked to decide the action]
- rst - any’ (3) [indicates that TCP RST bit will not be checked to decide the action]
- dscp - -1
- priority - 1

Example

```
Your Product (config-ext-nacl)# deny tcp 100.0.0.10
255.255.255.0 eq 20 any
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `permit tcp` - Specifies the TCP packets to be forwarded based on the associated parameters
- `show access-lists` - Displays the access list configuration

copy-to-cpu tcp

Command Objective This command copies the TCP control packets to control plane CPU with or without switching of packets based on the configured parameters.

Syntax **copy-to-cpu tcp {any | host <src-ip-address> | <src-ip- address> <src-mask> } [{gt <port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] {any | host <dest-ip-address> | <dest-ip-address> <dest- mask> } [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}|dscp <value (0-63)>}] [priority <value(1-255)>] [noswitching]**

Parameter Description

- `any | host <src-ip-address> | <src-ip-address> <src-mask>` - Copies the TCP control packets to control plane CPU with or without switching of packets based on the following source address configuration:
  - `any` - Copies all control packets. Does not check for the source IP address in the packets.
  - `host` - Copies only the control packets having the specified unicast host network IP address as the source address.
  - `<src-ip-address> <src-mask>` - Copies only the control packets having the specified unicast source IP address and mask.
- `gt` - Copies only the TCP control packets having the TCP source / destination port numbers greater than the specified port number. This value ranges between 1 and 65535.
- `lt` - Copies only the TCP control packets having the TCP source / destination port numbers lesser than the specified port number. This value ranges between 1 and 65535.
- `eq` - Copies only the TCP control packets having the specified TCP source / destination port numbers. This value ranges between 1 and 65535.
- `range` - Copies only the TCP control packets having the TCP source / destination port numbers within the specified range. This value ranges between 1 and 65535. This value specifies the minimum port number and the maximum port number values.
- `any | host <dest-ip-address> | <dest-ip-address> <dest- mask>` - Copies the TCP control packets to control plane CPU with or without switching of packets based on the following destination address configuration:
  - `any` - Copies all control packets. Does not check for the destination IP address in the packets.

  - `host` - Copies only the control packets having the specified host network IP address as the destination address.
  - `<dest-ip-address> <dest-mask>` - Copies only the control packets having the specified destination IP address and mask.
- `ack | rst` - Copies the TCP control packets to control plane CPU with or without switching of packets based on the following configuration:
  - `ack` - Copies only the control packets having the ACK bit set.
  - `rst` - Copies only the control packets having the RST bit set.
- `tos` - Copies the TCP control packets to control plane CPU with or without switching of packets based on the following type of service configuration:
  - `max-reliability` - Copies only the control packets having TOS field set as high reliability.
  - `max-throughput` - Copies only the control packets having TOS field set as high throughput.
  - `min-delay` - Copies only the control packets having TOS field set as low delay.
  - `normal` - Copies all control packets. Does not check for the TOS field in the packets.
  - `<value (0-7)>` - Copies the control packets based on the TOS value set. The value ranges between 0 and 7. This value represents different combination of TOS.
    - `0` - Copies all control packets. Does not check for the TOS field in the packets.
    - `1` - Copies only the control packets having TOS field set as high reliability.
    - `2` - Copies only the control packets having TOS field set as high throughput.
    - `3` - Copies the control packets having TOS field set either as high reliability or high throughput.
    - `4` - Copies only the control packets having TOS field set as low delay.
    - `5` - Copies the control packets having TOS field set either as low delay or high reliability.
    - `6` - Copies the control packets having TOS field set either as low delay or high throughput.
    - `7` - Copies the control packets having TOS field set either as low delay or high reliability or high throughput.
- `dscp` - Copies only the TCP control packets having the specified DSCP value. This value ranges between 0 and 63.
- `priority` - Copies only the TCP control packets having the specified L2 priority value. This value ranges between 1 and 255.
- `noswitching` - Copies the TCP control packets to control plane CPU without switching of packets.

Note: This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults

- any | host <src-ip-address> | <src-ip-address> <src-mask> - any
- gt - 0 (that is, the packets are not checked for TCP port number)
- lt - 0 (that is, the packets are not checked for TCP port number)

- eq - 0 (that is, the packets are not checked for TCP port number)
- range - 0 for minimum port number, 65535 for maximum port number.
- ack - any (that is, the packets are not checked for ACK bit)
- rst - any (that is, the packets are not checked for RST bit)
- any | host <dest-ip-address> | <dest-ip-address> <dest-mask> - any
- dscp - -1 (that is, the packets are not checked for DSCP value)
- priority – 1 The TCP port number details can be set either for source or destination. The default value is applied for destination TCP port number, if the source TCP port number is configured or vice-versa.

Example

```
Your Product (config-ext-nacl)# copy-to-cpu tcp any eq 300 any tos 1
priority 2 noswitching
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `show access-lists` - Displays the access lists configuration.

permit udp

Command Objective This command specifies the UDP packets to be forwarded based on the associated parameters.

Syntax **permit udp { any | host <src-ip-address> | <src-ip- address> <src-mask>}[{gt <port-number (1-65535)> | lt <port-number (1-65535)>| eq <port-number (1-65535)> |range <port-number (1-65535)> <port-number (1-65535)>}]{ any | host <dest-ip-address> | <dest-ip-address> <dest- mask> }[{ gt <port-number (1-65535)> | lt <port-number (1-65535)>| eq <port-number (1-65535)>| range <port-number (1-65535)> <port-number (1-65535)>}][{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp {<value (0-63)>}] [priority <(1-255)>]**

Parameter Description

- udp - User Datagram Protocol
- any| host <src-ip-address>|<src-ip-address><src-mask> - Source IP address can be
  - 'any' or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is from and the network mask to use with the source address
- port-number - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.
  - eq=equal
  - lt=less than
  - gt=greater than
  - range=a range of ports; two different port numbers must be specified
- any|host <dest-ip-address>|<dest-ip-address> <dest- mask> - Destination IP address can be
  - 'any' or

    - the word 'host' and the dotted decimal address or
    - number of the network or the host that the packet is destined for and the network mask to use with the destination address
- tos {max-reliability | max-throughput | min-delay | normal | <value (0-7)> | dscp <value(0-63)>} - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7.
- dscp - Differentiated services code point provides the quality of service control. The various options available are:
    - 0-63 - Differentiated services code point value
- priority - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

  Note: This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults

- dscp - -1
- priority - 1
- precedence - 1

Example

```
Your Product (config-ext-nacl)# permit udp any 100.0.0.10 load-balance src-
ip
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `deny udp` - Specifies the UDP packets to be rejected based on the associated parameters
- `show access-lists` - Displays the access list configuration

deny udp

Command Objective This command specifies the UDP packets to be rejected based on the associated parameters.

Syntax **deny udp { any | host <src-ip-address> | <src-ip-address> <src-mask>}[{gt <port-number (1-65535)> | lt <port-number (1-65535)>| eq <port-number (1-65535)> | range<port-number (1-65535)> <port-number (1-65535)>}]{ any | host <dest-ip-address> | <dest-ip-address> <dest-mask> }[{ gt<port-number (1-65535)> | lt<port-number (1-65535)>| eq<port-number (1-65535)>| range <port-number (1-65535)> <port-number (1-65535)>}][{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp {<value (0-63)>}] [priority <(1-255)>]**

Parameter Description

- udp - User Datagram Protocol
- any| host <src-ip-address>|<src-ip-address><src-mask> - Source IP address can be
  - 'any' or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is from and the network mask to use with the source address
- port-number - Port Number. The input for the source and the destination port-number is prefixed with one of the following operators.
  - eq=equal
  - lt=less than
  - gt=greater than
  - range=a range of ports; two different port numbers must be specified
- any|host<dest-ip-address>|<dest-ip-address><dest-mask> - Destination IP address can be
  - 'any' or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is destined for and the network mask to use with the destination address
- tos - Type of service. Can be max-reliability, max throughput, min-delay, normal or a range of values from 0 to 7, Differentiated Services Code Point (DSCP) values to match against incoming packets.
- dscp - Differentiated services code point provides the quality of service control. The various options available are:
  - 0-63 - Differentiated services code point value
- priority - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

  Note: This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults

- dscp - -1
- priority - 1
- precedence - 1

Example

```
Your Product (config-ext-nacl)# deny udp host 10.0.0.1 any eq 20
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `permit udp` - Specifies the UDP packets to be forwarded based on the associated parameters
- `show access-lists` - Displays the access list configuration

copy-to-cpu udp

Command Objective This command copies the UDP control packets to control plane CPU with or without switching of packets based on the configured parameters.

Syntax **copy-to-cpu udp { any | host <src-ip-address> | <src-ip- address> <src-mask>} [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host <dest-ip-address> | <dest-ip-address> <dest- mask> } [{ gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port- number (1-65535)> <port-number (1-65535)>}] [{tos{max- reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}] [priority <(1-255)>] [noswitching]**

Parameter Description

- `any | host <src-ip-address> | <src-ip-address> <src-mask>` - Copies the UDP control packets to control plane CPU with or without switching of packets based on the following source address configuration:
    - `any` - Copies all control packets. Does not check for the source IP address in the packets.
    - `host` - Copies only the control packets having the specified unicast host network IP address as the source address.
    - `<src-ip-address> <src-mask>` - Copies only the control packets having the specified unicast source IP address and mask.
- `gt` - Copies only the UDP control packets having the UDP source / destination port numbers greater than the specified port number. This value ranges between 1 and 65535.
- `lt` - Copies only the UDP control packets having the UDP source / destination port numbers lesser than the specified port number. This value ranges between 1 and 65535.
- `eq` - Copies only the UDP control packets having the specified UDP source / destination port numbers. This value ranges between 1 and 65535.
- `range` - Copies only the UDP control packets having the UDP source / destination port numbers within the specified range. This value ranges between 1 and 65535. This value specifies the minimum port number and the maximum port number values.
- `any | host <dest-ip-address> | <dest-ip-address> <dest- mask>` - Copies the UDP control packets to control plane CPU with or without switching of packets based on the following destination address configuration:
    - `any` - Copies all control packets. Does not check for the destination IP address in the packets.
    - `host` - Copies only the control packets having the specified host network IP address as the destination address.
    - `<dest-ip-address> <dest-mask>` - Copies only the control packets having the specified destination IP address and mask.
- `ack | rst` - Copies the UDP control packets to control plane CPU with or without switching of packets based on the following configuration:
    - `ack` - Copies only the control packets having the ACK bit set.
    - `rst` - Copies only the control packets having the RST bit set.
- `tos` - Copies the UDP control packets to control plane CPU with or without switching of packets

based on the following type of service configuration:

- max-reliability - Copies only the control packets having TOS field set as high reliability.
- max-throughput - Copies only the control packets having TOS field set as high throughput.
- min-delay - Copies only the control packets having TOS field set as low delay.
- normal - Copies all control packets. Does not check for the TOS field in the packets.
- <value (0-7)> - Copies the control packets based on the TOS value set. The value ranges between 0 and 7. This value represents different combination of TOS.
    - 0 - Copies all control packets. Does not check for the TOS field in the packets.
    - 1 - Copies only the control packets having TOS field set as high reliability.
    - 2 - Copies only the control packets having TOS field set as high throughput.
    - 3 - Copies the control packets having TOS field set either as high reliability or high throughput.
    - 4 - Copies only the control packets having TOS field set as low delay.
    - 5 - Copies the control packets having TOS field set either as low delay or high reliability.
    - 6 - Copies the control packets having TOS field set either as low delay or high throughput.
    - 7 - Copies the control packets having TOS field set either as low delay or high reliability or high throughput.

- dscp - Copies only the UDP control packets having the specified DSCP value. This value ranges between 0 and 63.
- priority - Copies only the UDP control packets having the specified L2 priority value. This value ranges between 1 and 255.
- noswitching - Copies the UDP control packets to control plane CPU without switching of packets. **Note:** This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults

- any | host <src-ip-address> | <src-ip-address> <src-mask> - any
- gt - 0 (that is, the packets are not checked for UDP port number)
- lt - 0 (that is, the packets are not checked for UDP port number)
- eq - 0 (that is, the packets are not checked for UDP port number)
- range - 0 for minimum port number. 65535 for maximum port number.
- any | host <dest-ip-address> | <dest-ip-address> <dest-mask> - any
- dscp - -1 (that is, the packets are not checked for DSCP value)
- priority - 1

Note: The UDP port number details can be set either for source or destination. The default value is applied for destination UDP port number, if the source UDP port number is configured or vice-versa.

Example

```
Your Product (config-ext-nacl)# copy-to-cpu udp any eq 300 any tos 1
priority 2 noswitching
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `show access-lists` - Displays the access lists configuration.

permit icmp

Command Objective This command specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.

Syntax **permit icmp {any |host <src-ip-address>|<src-ip-address> <mask>}{any | host <dest-ip-address> | <dest-ip-address> <mask> }[<message-type (0-255)>] [<message-code (0-255)>] [priority <(1-255)>]**

Parameter Description

- `icmp` - Internet Control Message Protocol
- `any| host<src-ip-address>|<src-ip-address> <mask>` - Source IP address can be
  - 'any' or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is from and the network mask to use with the source address
- `any|host <dest-ip-address>|<dest-ip-address><mask>` - Destination IP address can be
  - 'any' or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is destined for and the network mask to use with the destination address
- `message-type` - Message type

Value	**ICMP type**
0	Echo reply
3	Destination unreachable
4	Source quench
5	Redirect
8	Echo request
11	Time exceeded
12	Parameter problem
13	Timestamp request
14	Timestamp reply

15	Information request
16	Information reply
17	Address mask request
18	Address mask reply
155	No ICMP type

- `message-code` - ICMP Message code

Value	ICMP code
0	Network unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
4	Fragment need
5	Source route fail
6	Destination network unknown
7	Destination host unknown
8	Source host isolated
9	Destination network administratively prohibited
10	Destination host administratively prohibited
11	Network unreachable TOS
12	Host unreachable TOS
255	No ICMP code

- `priority` - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

  Note: This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults

- message-type/message code - 255
- priority - 1

Example

```
Your Product (config-ext-nacl)# permit icmp any 10.0.0.1 load balance src-
ip
```

Related Command(s)

- `ip access-list` - Created IP ACLs and enters the IP Access-list configuration mode
- `deny icmp` - Specifies the ICMP packets to be rejected based on the IP address and associated parameters
- `show access-lists` - Displays the access list configuration

deny icmp

Command Objective This command specifies the ICMP packets to be rejected based on the IP address and associated parameters.

Syntax **deny icmp {any |host <src-ip-address>|<src-ip-address> <mask>}{any | host <dest-ip-address> | <dest-ip-address> <mask> }[<message-type (0-255)>] [<message-code (0-255)>] [priority <(1-255)>]**

Parameter Description

- `icmp` - Internet Control Message Protocol
- `any | host<src-ip-address> | <src-ip-address> <mask>` - Source IP address can be
  - 'any' or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is from and the network mask to use with the source address
- `any | host <dest-ip-address>| <dest-ip-address> <mask>` - Destination IP address can be
  - 'any' or
  - the word 'host' and the dotted decimal address or
  - number of the network or the host that the packet is destined for and the network mask to use with the destination address
- `message-type` - Message type

Value	ICMP type
0	Echo reply
3	Destination unreachable
4	Source quench
5	Redirect

8	Echo request
11	Time exceeded
12	Parameter problem
13	Timestamp request
14	Timestamp reply
15	Information request
16	Information reply
17	Address mask request
18	Address mask reply
155	No ICMP type

- `message-code` - ICMP Message code

Value	**ICMP code**
0	Network unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
4	Fragment need
5	Source route fail
6	Destination network unknown
7	Destination host unknown
8	Source host isolated
9	Destination network administratively prohibited
10	Destination host administratively prohibited
11	Network unreachable TOS
12	Host unreachable TOS
255	No ICMP code

- `priority` - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

Note: This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults

- message-type / message code - 255
- priority - 1

Example

```
Your Product (config-ext-nacl)# deny icmp host 100.0.0.10
10.0.0.1 255.255.255.255
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `permit icmp` - Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters
- `show access-lists` - Displays the access list configuration

copy-to-cpu icmp

Command Objective This command copies the ICMP control packets to control plane CPU with or without switching of packets based on the configured parameters.

Syntax **copy-to-cpu icmp {any |host <src-ip-address>|<src-ip- address> <mask>} {any | host <dest-ip-address> | <dest-ip- address> <mask> } [<message-type (0-255)>] [<message-code (0-255)>] [priority <(1-255)>] [noswitching**]

Parameter Description

- `any |host <src-ip-address>|<src-ip-address> <mask>` - Copies the ICMP control packets to control plane CPU with or without switching of packets based on the following source address configuration:
  - `any` - Copies all control packets. Does not check for the source IP address in the packets.
  - `host` - Copies only the control packets having the specified unicast host network IP address as the source address.
  - `<src-ip-address> <mask>` - Copies only the control packets having the specified unicast source IP address and mask.
- `any | host <dest-ip-address> | <dest-ip-address> <mask>` - Copies the ICMP control packets to control plane CPU with or without switching of packets based on the following destination address configuration:
  - `any` - Copies all control packets. Does not check for the destination IP address in the packets.

    - `host` - Copies only the control packets having the specified host network IP address as the destination address.
    - `<dest-ip-address> <mask>` - Copies only the control packets having the specified destination IP address and mask.
- `<message-type (0-255)>` - Copies only the ICMP control packets having the specified message type. This value ranges between 0 and 255. The value can be one of the following:

Value	**ICMP Type**
0	Echo reply
3	Destination unreachable
4	Source quench
5	Redirect
8	Echo request
11	Time exceeded
12	Parameter problem
13	Timestamp request
14	Timestamp reply
15	Information request
16	Information reply
17	Address mask request
18	Address mask reply

- `<message-code (0-255)>` - Copies only the ICMP control packets having the specified message code. This value ranges between 0 and 255. The value can be one of the following:

Value	ICMP Code
0	Network unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
4	Fragment need
5	Source route failed

6	Destination network unknown
7	Destination host unknown
8	Source host isolated
9	Destination network administratively prohibited
10	Destination host administratively prohibited
11	Network unreachable TOS
12	Host unreachable TOS
255	No ICMP codes to be filtered

- `priority <(1-255)>` - Copies only the ICMP control packets having the specified L2 priority value. This value ranges between 1 and 255.
- `noswitching` - Copies the UDP control packets to control plane CPU without switching of packets.

  Note: This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults

- any |host <src-ip-address>|<src-ip-address> <mask> - any
- any | host <dest-ip-address> | <dest-ip-address> <mask> - any
- priority - 1

Example

```
Your Product (config-ext-nacl)# copy-to-cpu icmp any any 11 7 noswitching
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `show access-lists` - Displays the access lists configuration.

permit icmpv6

Command Objective This command specifies the ICMPv6 packets to be forwarded based on the IP address and the associated parameters.

Syntax **permit icmpv6 {any | host <src-ipv6-addr> <src-prefix-len (0-128)>} {any | host <dst-ipv6-addr> <dst-prefix-len (0-128)} [<message-type (0-255)>] [<message-code (0-255)>] [dscp <value (0-63)>] [flow-label <value (0-1048575)>] [priority <value (1-7)>]**

Parameter Description

- `icmpv6` - Internet Control Message Protocol Version 6

- `any | host <src-ipv6-addr> <src-prefix-len (0-128)>-`
- `any | host <dst-ipv6-addr> <dst-prefix-len (0-128)-`
- `message-type` - Message type, refer to RFC4443
- `message-code` - ICMPv6 Message code, refer to RFC4443
- `priority` - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

  Note: This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults

- message-type/message code - 255
- priority - 1

Example

Related Command(s) `show access-lists` - Displays the access lists configuration.

deny icmpv6

Command Objective This command specifies the ICMPv6 packets to be rejected based on the IP address and associated parameters.

Syntax **deny icmpv6 {any | host <src-ipv6-addr> <src-prefix-len (0-128)>} {any | host <dst-ipv6-addr> <dst-prefix-len (0-128)} [<message-type (0-255)>] [<message-code (0-255)>] [dscp <value (0-63)>] [flow-label <value (0-1048575)>] [priority <value (1-7)>]**

Parameter Description

- `icmpv6` - Internet Control Message Protocol Version 6
- `any | host <src-ipv6-addr> <src-prefix-len (0-128)>-`
- `any | host <dst-ipv6-addr> <dst-prefix-len (0-128)-`
- `message-type` - Message type, refer to RFC4443
- `message-code` - ICMPv6 Message code, refer to RC4443
- `priority` - The priority of the filter used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.

Note: This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults

- message-type / message code – 255
- priority - 1

Example

Related Command(s) `show access-lists` - Displays the access lists configuration.

copy-to-cpu icmpv6

Command Objective This command copies the ICMPv6 control packets to control plane CPU with or without switching of packets based on the configured parameters.

Syntax **copy-to-cpu icmpv6 {any | host <src-ipv6-addr> <src- prefix-len (0-128)} {any | host <dst-ipv6-addr> <dst- prefix-len (0-128)>} [<message-type (0-255)>] [<message- code (0-255)>] [dscp <value (0-63)>] [flow-label <value (0-1048575)>] [priority <value (1-7)>] [noswitching]**

Parameter Description

- `<message-type (0-255)>` - Copies only the ICMP control packets having the specified message type. This value ranges between 0 and 255. The value can be one of the following:

Value	ICMP Type
0	Reserved
1	Destination unreachable
3	Time Exceeded
4	Parameter Problem
128	Echo Request
129	Echo Reply
130	Multicast Listener Query
131	Multicast Listener Report
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect Message
139	ICMP Node Information Query
140	ICMP Node Information Response

- `<message-code (0-255)>` - Copies only the ICMP control packets having the specified message code. This value ranges between 0 and 255. The value can be one of the following:

Value	ICMP Code
0	No Route to Destination
1	Communication with Destination Administratively Prohibited
2	Beyond Scope of Source Address
3	Address Unreachable
4	Port Unreachable
5	Source Address Failed Ingress/Egress Policy
6	Reject Route to Destination
255	Sequence Number Reset

- `priority` - Copies only the UDP control packets having the specified L2 priority value. This value ranges between 1 and 255.
- `noswitching` - Copies the UDP control packets to control plane CPU without switching of packets.

  Note: This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults

- message-type / message code - 255
- priority - 1

Example

Related Command(s) `s. how access-lists` - Displays the access lists configuration.

ip access-group

Command Objective This command enables access control for the packets on the interface. It controls access to a Layer 2 or Layer 3 interface.

The no form of this command removes all access groups or the specified access group from the interface. The direction of filtering is specified using the token in or out.

Syntax **ip access-group <access-list-number (1-65535)> {in | out}**

no ip access-group [<access-list-number (1-65535)>] {in | out}

Parameter Description

- `access-list-number` - IP access control list number

- `in` - Inbound packets
- `out` - Outbound packets

Mode Interface Configuration Mode

Notes:

- IP access list must have been created
- The out port only supports one single port.
- Following are the limitations for this command to be applicable to Layer 2 interfaces.
    - An IP ACL applied to a Layer 2 interface filters only the IP packets. MAC access-group interface configuration command with MAC extended ACLs must be used to filter non-IP packets.

Example

```
Your Product (config-if)# ip access-group 1 in
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `show access-lists` - Displays the access list configuration

mac access-group

Command Objective This command applies a MAC access control list (ACL) to a Layer 2 interface.

The no form of this command can be used to remove the MAC ACLs from the interface. The direction of filtering is specified using the token in or out.

Syntax **mac access-group <access-list-number (1-65535)> {in | out}**

no mac access-group [<access-list-number (1-65535)>] {in | out}

Parameter Description

- `access-list-number` - Access List Number
- `in` - Inbound packets
- `out` - Outbound packets

Mode Interface Configuration Mode

Notes:

- MAC access list must have been created.
- The out port only supports one single port.

Example

```
Your Product (config-if)# mac access-group 5 in
```

Related Command(s)

- `mac access-list extended` - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- `permit - MAC` - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- `deny - MAC` - Specifies the packets to be rejected based on the MAC address and the associated parameters.
- `show access-lists` - Displays the access list statistics

permit - MAC

Command Objective This command specifies the packets to be forwarded based on the MAC address and the associated parameters, that is, this command allows non-IP traffic to be forwarded if the conditions are matched.

Syntax **permit { any | host <src-mac-address>}{ any | host <dest- mac-address> }[aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines- echo | vines-ip | xns-id | <protocol (0-65535)> | type <0-65535> <0-65535> | lsap <0-65535> <0-65535>][encaptype <value (1-65535)>][Vlan <vlan-id (1-4094)>][priority <value (1-255)>]**

Parameter Description

- `any | host <src-mac-address >` - Source MAC address to be matched with the packet
- `any | host <dest-mac-address >` - Destination MAC address to be matched with the packet
- `aarp` - Ethertype AppleTalk Address Resolution Protocol that maps a data- link address to a network address
- `amber` - EtherType DEC-Amber
- `dec-spanning` - EtherType Digital Equipment Corporation (DEC) spanning tree
- `decnet-iv` - EtherType DECnet Phase IV protocol
- `diagnostic` - EtherType DEC-Diagnostic
- `dsm` - EtherType DEC-DSM/DDP
- `etype-6000` - EtherType 0x6000
- `etype-8042` - EtherType 0x8042
- `lat` - EtherType DEC-LAT
- `lavc-sca` - EtherType DEC-LAVC-SCA
- `mop-console` - EtherType DEC-MOP Remote Console
- `mop-dump` - EtherType DEC-MOP Dump
- `msdos` - EtherType DEC-MSDOS
- `mumps` - EtherType DEC-MUMPS
- `netbios` - EtherType DEC- Network Basic Input/Output System (NETBIOS)
- `vines-echo` - EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems
- `vines-ip` - EtherType VINES IP
- `xns-id` - EtherType Xerox Network Systems (XNS) protocol suite

- `<protocol (0-65535)>` - Specifies the non-IP protocol type to be filtered. The value ranges between 0 and 65535. The value 0 represents that filter is applicable for all protocols.
- `type` - Specifies the ether type value and its mask. The value ranges between 0 and 65535 for type value and mask. The mask feature is currently not supported.
- `lsap` - Specifies the LSAP value and its mask. The value ranges between 0 and 65535 for type value and mask. The mask feature is currently not supported.
- `encaptype` - Encapsulation Type

Mode ACL MAC Configuration Mode

Defaults

- <protocol (0-65535)> - 0
- sub-action - none
- vlan-id - 0
- priority - 1
- outerEtherType - 0

Notes: MAC access list must have been created.

Example

```
Your Product (config-ext-macl)# permit host 00:11:22:33:44:55 any load-
balance src-ip vlan-action modify lan 526
```

Related Command(s)

- `mac access-list extended` - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- `user-defined access-list` - Creates the user defined access-list.
- `mac access-group` - Applies a MAC access control list (ACL) to a Layer 2 interface
- `deny - MAC` - Specifies the packets to be rejected based on the MAC address and the associated parameters
- `show access-lists` - Displays the access list statistics

deny - MAC

Command Objective This command specifies the packets to be rejected based on the MAC address and the associated parameters.

Syntax **deny { any | host <src-mac-address>}{ any | host <dest- mac-address> }[aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc- sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-id | <protocol (0-65535)> | type <0-65535> <0-65535> | lsap <0-65535> <0-65535>][encaptype <value (1-65535)>][Vlan <vlan-id (1-4094)>][priority <value (1-255)>]**

Parameter Description

- `any | host <src-mac-address >` - Source MAC address to be matched with the packet

- `any | host <dest-mac-address >` - Destination MAC address to be matched with the packet
- `aarp` - Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address
- `amber` - EtherType DEC-Amber
- `dec-spanning` - EtherType Digital Equipment Corporation (DEC) spanning tree
- `decent-iv` - EtherType DECnet Phase IV protocol
- `diagnostic` - EtherType DEC-Diagnostic
- `dsm` - EtherType DEC-DSM/DDP
- `etype-6000` - EtherType 0x6000
- `etype-8042` - EtherType 0x8042
- `lat` - EtherType DEC-LAT
- `lavc-sca` - EtherType DEC-LAVC-SCA
- `mop-console` - EtherType DEC-MOP Remote Console
- `mop-dump` - EtherType DEC-MOP Dump
- `msdos` - EtherType DEC-MSDOS
- `mumps` - EtherType DEC-MUMPS
- `netbios` - EtherType DEC- Network Basic Input/Output System (NETBIOS)
- `vines-echo` - EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems
- `vines-ip` - EtherType VINES IP
- `xns-id` - EtherType Xerox Network Systems (XNS) protocol suite
- `<protocol (0-65535)>` - Specifies the non-IP protocol type to be filtered. The value ranges between 0 and 65535. The value 0 represents that filter is applicable for all protocols.
- `type` - Specifies the ether type value and its mask. The value ranges between 0 and 65535 for type value and mask. The mask feature is currently not supported.
- `lsap` - Specifies the LSAP value and its mask. The value ranges between 0 and 65535 for type value and mask. The mask feature is currently not supported.
- `encaptype` - Encapsulation Type
- `vlan` - VLAN ID to be filtered
- `priority` - The priority of the L2 filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. Higher value of 'filter priority' implies a higher priority.
- `outerEtherType` - EtherType value to match on Service vlan tag

Mode ACL MAC Configuration Mode

Defaults

- <protocol (0-65535)> - 0
- vlan-id - 0
- priority - 1
- outerEtherType - 0

Notes: MAC access list must have been created.

Example

```
Your Product (config-ext-macl)# deny any host 00:11:22:33:44:55 priority
```

```
200
```

Related Command(s)

- `mac access-list extended` - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- `user-defined access-list` - Creates the user defined access-list.
- `mac access-group` - Applies a MAC access control list (ACL) to a Layer 2 interface
- `permit - MAC` - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- `show access-lists` - Displays the access list statistics

copy-to-cpu - MAC

Command Objective This command copies the MAC protocol control packets to control plane CPU with or without switching of packets based on the configured parameters.

Syntax **copy-to-cpu { any | host <src-mac-address>}{ any | host <dest-mac-address> } [aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 |etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-id | <protocol (0-65535)> | type <(0-65535)> <(0-65535)> | lsap <(0-65535)> <(0-65535)>] [encaptype <value (1-65535)>][Vlan <vlan-id (1-4094)>] [priority <value (1-255)>] [noswitching]**

Parameter Description

- `any | host <src-mac-address>` - Copies the MAC protocol control packets to control plane CPU with or without switching of packets based on the following source address configuration:
  - `any` - Copies all control packets. Does not check for the source MAC address in the packets.
  - `host` - Copies only the control packets having the specified source MAC address.
- `any | host <dest-mac-address>` - Copies the MAC protocol control packets to control plane CPU with or without switching of packets based on the following destination address configuration:
  - `any` - Copies all control packets. Does not check for the destination MAC address in the packets.
  - `host` - Copies only the control packets having the specified destination MAC address.
- `aarp` - Copies only the MAC protocol control packets having the protocol type as AARP.
- `amber` - Copies only the MAC protocol control packets having the protocol type as DEC-Amber.
- `dec-spanning` - Copies only the MAC protocol control packets having the protocol type as DEC spanning tree.
- `decnet-iv` - Copies only the MAC protocol control packets having the protocol type as DECnet Phase IV.
- `diagnostic` - Copies only the MAC protocol control packets having the protocol type as DEC-diagnostic.
- `dsm` - Copies only the MAC protocol control packets having the protocol type as DEC-DSM / DDP.
- `etype-6000` - Copies only the MAC protocol control packets having the protocol type as EtherType

0x6000.

- `etype-8042` - Copies only the MAC protocol control packets having the protocol type as EtherType 0x8042.
- `lat` - Copies only the MAC protocol control packets having the protocol type as DEC-LAT.
- `lavc-sca` - Copies only the MAC protocol control packets having the protocol type as DEC-LAVC-SCA.
- `mop-console` - Copies only the MAC protocol control packets having the protocol type as DEC-MOP remote console.
- `mop-dump` - Copies only the MAC protocol control packets having the protocol type as DEC-MOP Dump.
- `msdos` - Copies only the MAC protocol control packets having the protocol type as DEC-MSDOS.
- `mumps` - Copies only the MAC protocol control packets having the protocol type as DEC-MUMPS.
- `netbios` - Copies only the MAC protocol control packets having the protocol type as NETBIOS.
- `vines-echo` - Copies only the MAC protocol control packets having the protocol type as VINES Echo.
- `vines-ip` - Copies only the MAC protocol control packets having the protocol type as VINES IP.
- `xns-id` - Copies only the MAC protocol control packets having the protocol type as XNS protocol suite.
- `<protocol (0-65535)>` - Copies only the MAC protocol control packets having the specified non-IP protocol type value. This value ranges between 0 and 65535.
- `type` - Copies only the MAC protocol control packets having the specified ether type value and mask. The value ranges between 0 and 65535 for type value and mask. The mask feature is currently not supported.
- `lsap` - Copies only the MAC protocol control packets having the specified LSAP value and mask. The value ranges between 0 and 65535 for type value and mask. The mask feature is currently not supported.
- `encaptype` - Copies only the MAC protocol control packets having the specified Ether Type value. This value ranges between 1 and 65535.
- `Vlan` - Copies only the MAC protocol control packets having the specified VLAN ID. This value ranges between 1 and 4094.
- `priority` - Copies only the MAC protocol control packets having the specified L2 priority value. This value ranges between 1 and 255.
- `noswitching` - Copies the MAC protocol control packets to control plane CPU without switching of packets.

  Note: This parameter is not supported in some models.

Mode ACL MAC Configuration Mode

Defaults

- any | host <src-mac-address> - any
- any | host <dest-mac-address> - any
- <protocol (0-65535)> - 0
- encaptype - 0 (that is, the packets are not checked for Ether Type)

- Vlan - 0 (that is, the packets are not checked for VLAN ID)
- priority - 1
- outerEtherType - 0 (that is, the packets are not checked for outer Ether type)

Example `Your Product (config-ext-macl)# copy-to-cpu any any aarp encaptype 10`

Related Command(s)

- `mac access-list extended` - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- `show access-lists` - Displays the access list statistics

show access-lists

Command Objective This command displays the access lists configuration.

Syntax **show access-lists [[{ip | mac}] <access-list-number (1-65535)>]**

Parameter Description

- `ip` - IP Access List
- `mac` - MAC Access List

Mode Privileged/User EXEC Mode

Example

```
Your Product# show access-lists
EIP ACCESS LISTS
-----------------------------------------------------------------
Standard IP Access List 34
-----------------------------------------------------------------
IP address Type                  : IPV4
Source IP address                : 172.30.3.134
Source IP address mask           : 255.255.255.25
Source IP Prefix Length          : 32
Destination IP address           : 0.0.0.0
Destination IP address mask      : 0.0.0.0
Destination IP Prefix Length     : 0
Flow Identifier                  : 0
In Port List                     : NIL
Out Port List                    : NIL
Filter Action                    : Deny
Status                            : InActive
Extended IP Access List 1002
---------------------------------------------------------
Filter Priority                  : 1
Filter Protocol Type             : ANY
IP address Type                  : IPV4
Source IP address                : 0.0.0.0
Source IP address mask           : 0.0.0.0
Source IP Prefix Length          : 0
```

```
Destination   IP   address   :   0.0.0.0
Destination  IP  address  mask  :  0.0.0.0
Destination IP Prefix Length : 0
Flow Identifier                 : 0
In Port List                    : NIL
Out Port List                   : NIL
Filter TOS                      : Invalid combination
Filter DSCP                     : NIL
Filter Action                   :
Permit Status                   : InActive
Extended IP Access List 10022
-----------------------------------------------------------------
Filter Priority                 : 1
Filter Protocol Type            : ANY
IP address Type                 : IPV4
Source IP address               : 0.0.0.0
Source IP address mask          : 0.0.0.0
Source IP Prefix Length         : 0
Destination IP address          : 0.0.0.0
Destination IP address mask     : 0.0.0.0
Destination IP Prefix Length    : 0
Flow Identifier                 : 0
In Port List                    : NIL
Out Port List                   : NIL
Filter TOS                      : Invalid combination
Filter DSCP                     : NIL
Filter Action                   : Permit
Status                          : InActive
MAC ACCESS LISTS
-----------------------------
No MAC Access Lists have been configured
```

Related Command(s)

- `ip access-list` - Creates IP ACLs and enters the IP Access-list configuration mode
- `mac access-list extended` - Creates Layer 2 MAC ACLs, and returns the MAC-Access list configuration mode to the user
- `permit – standard mode` - Specifies the packets to be forwarded depending upon the associated parameters
- `deny – standard mode` - Denies traffic if the conditions defined in the deny statement are matched
- `permit- ip/ospf/pim/protocol type` - Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched
- `deny – ip/ospf/pim/protocol type` - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched
- `permit tcp` - Specifies the TCP packets to be forwarded based on the associated parameters
- `deny tcp` - Specifies the TCP packets to be rejected based on the associated parameters
- `permit udp` - Specifies the UDP packets to be forwarded based on the associated parameters
- `deny udp` - Specifies the UDP packets to be rejected based on the associated parameters
- `permit icmp` - Specifies the ICMP packets to be forwarded based on the IP address and the

associated parameters

- `deny icmp` - Specifies the ICMP packets to be rejected based on the IP address and associated parameters
- `ip access-group` - Enables access control for the packets on the interface
- `mac access-group` - Applies a MAC access control list (ACL) to a Layer 2 interface
- `permit` - Specifies the packets to be forwarded based on the MAC address and the associated parameters
- `deny` - specifies the packets to be rejected based on the MAC address and the associated parameters

storm-control

Command Objective This command sets the storm control rate for broadcast, multicast and DLF packets.

The no form of the command sets storm control rate for broadcast, multicast and DLF packets to the default value.

Syntax **storm-control { broadcast |multicast | dlf } level <rate- value>**
no storm-control { broadcast |multicast | dlf } level

Parameter Description

- `broadcast` - Broadcast packets
- `multicast` - Multicast packets
- `dlf` - Unicast packets
- `level` - Storm-control suppression level as a total number of packets per second.

Mode Interface Configuration Mode

Defaults Broadcast, multicast, and dlf storm control are disabled.

Example

```
Your Product(config-if)# storm-control broadcast level 1000
```

Notes:

- The rate must be specified in terms of packets per second
- Storm control is supported only on physical interfaces

Related Command(s) `show interfaces` - Displays the interface status and configuration

rate-limit-output

Command Objective This command enables the rate limiting and burst size rate limiting by configuring the egress packet rate of an interface.

The no form of the command disables the rate limiting and burst size rate limiting on an egress port.

Syntax **rate-limit output [<rate-value>] [<burst-value>]**

no rate-limit output [rate-limit] [burst-limit]

Parameter Description

- `rate-value` - Line rate in kbps
- `burst-val`ue - Burst size value in kbps

Mode Interface Configuration Mode **Defaults**

- rate-value - 0
- burst-value - 0

Example

```
Your Product(config-if)# rate-limit output 64 32
```

29 DCBX

DCBX (Data Center Bridge capability eXchange protocol) refers to a procedure to determine the related traffic settings of the both link partners, to achieve the converged Ethernet with/without lossless feature.

There are several versions of DCBX, Supermicro switches implements the version of "DCB Capability Exchange Protocol Base Specification, Rev 1.01", also refer to CEE (Converged Enhanced Ethernet).

DCBX requires LLDP to carry its messages that exchanging between the both end of the link, hence the DCBX messages are actually in form of the LLDP TLVs, and practically the DCBX requires LLDP in operating.

Supermicro switches defined the DCBX configuration in two parts, one is the CEE-Map, and the other is the port advertisement settings. CEE-Maps defined the objects as the protocol specification required:

- Relationship between traffic priorities and priority-group,
- PFC (Priority-based Flow Control) feature for each priority,
- Bandwidth allocation in percentage for each priority-group.

And the ports (interfaces) must associate with a CEE-Map first, then configured the LLDP TLV settings for DCBX. With completely configured the CEE-Map and port settings, then the protocol can be started, to negotiate with the link partner, and automatically adjust the PFC and bandwidth allocation settings.

Since DCBX uses LLDP to negotiate and adjust PFC and bandwidth allocations, so it is required to remove all pause settings, scheduler settings, and rate limitations from the interface will start DCBX, to ensure the DCBX can work correctly.

The list of CLI commands for DCBX as follows:

- show cee-map
- show lldp dcbx interface
- cee-map
- group-bandwidth
- group
- pri2pg
- priority
- pfc group
- pfc priority
- cee
- dcbx cee
- lldp tlv-select dcbx-cee-pfc
- lldp tlv-select dcbx-cee-pg
- pfc

show cee-map

Command Objective This command lists the defined CEE-Maps in the system.

Syntax **show cee-map [<cee-map-id(1-4)>]**

Parameter Description `<cee-map-id(1-4)>`– Specify which CEE-Map to list, omitting the CEE-Map index to list all.

Mode

- Privileged EXEC Mode
- Global Configuration Mode

Example

```
SMIS# show cee-map
CEE-Map 1
Ports :
Priority  Group  PFC  Description
------------------------------------
       0      0   No  LAN
       1      0   No
       2      0   No
       3      1   Yes  FCoE/FIP
       4      0   No
       5      0   No
       6      0   No
       7      0   No
Group   Bandwidht(%)  PFC  Description
---------------------------------------
    0            20   No  LAN
    1            80   Yes  SAN
    2             0   No
    3             0    No
    4             0    No
    5             0    No
    6             0    No
    7             0    No
    15           MAX   No
 Application-Protocol-ID   Type       Protocol-ID    Priority
------------------------------------------------------------------------------------------------------------------------
                        1   ether-type 0x8906         3
                        2   ether-type 0x8914         3
                        3   tcp-udp    3260           4
```

Related Command(s) `cee-map` – Create or enter a CEE-Map to configure.

show lldp dcbx interface

Command Objective This command lists the interface status of the DCBX negotiation.

Syntax **show lldp dcbx interface [<iftype> <ifnum>]**

Mode

- Privileged EXEC Mode
- Global Configuration Mode

Example

```
SMIS# show lldp dcbx interface extreme-ethernet 0/58
Ex0/58:
DCBX Control Message Exchange Information
----------------------------------------------------------------------------------------
Status: Synchronized
Peer message seq#: 2 (acknowledged: 2)
Local message seq#: 2 (acknowledged: 2)
DCBX Feature Information
----------------------------------------------------------------------------------------
Feature: PG, Priority Groups
Type/subtype: 2/0
Enabled: Yes
Advertisement: Yes
Willing: Yes
Error: No
Operation status: Operational
Config (operation/desired/peer):
          PG0...20 / 20 / 20
          PG1...80 / 80 / 80
          PG2...0 / 0 / 0
          PG3...0 / 0 / 0
          PG4...0 / 0 / 0
          PG5...0 / 0 / 0
          PG6...0 / 0 / 0
          PG7...0 / 0 / 0
          PG15...MAX / MAX / MAX
```

```
         #TCs...8 / 8 / 8
Feature: PFC, Priority-based Flow Control
Type/subtype: 3/0
Enabled: Yes
Advertisement: Yes
Willing: Yes
Error: No
Operation status: Operational
Config (operation/desired.pg/peer):
         Pri0...0 / 0.0 / 0
         Pri1...0 / 0.0 / 0
         Pri2...0 / 0.0 / 0
         Pri3...1 / 1.1 / 1
         Pri4...0 / 0.0 / 0
         Pri5...0 / 0.0 / 0
         Pri6...0 / 0.0 / 0
         Pri7...0 / 0.0 / 0
         #TCs...8 / 8 / 8
Feature: Application Protocol
Type/subtype: 4/0
Enabled: Yes
Advertisement: Yes
Willing: No
Error: No
Operation status: Operational
Config (operation/desired/peer):
         Operation Config
         Type       Protocol-ID    Priority
         ----------------------------------
         ether-type 0x8906         3
         ether-type 0x8914         3
         tcp-udp    3260           4
         Desired Config
         Type       Protocol-ID    Priority
         ----------------------------------
         ether-type 0x8906         3
         ether-type 0x8914         3
         tcp-udp    3260           4
         Peer Config
         Type       Protocol-ID    Priority
         ----------------------------------
         ether-type 0x8906         3
         ether-type 0x8914         3
         tcp-udp    3260           4
```

Related Command(s)

- `cee` – Associate an interface with CEE-Map.
- `dcbx cee` – Start DCBX on an interface.
- `lldp tlv-select dcbx-cee-pfc` – Configure the transmitting PFC TLV.
- `lldp tlv-select dcbx-cee-pg` – Configure the transmitting PG TLV.

cee-map

Command Objective To create or enter a CEE-Map.

The no form of this command deletes a CEE-Map.

Syntax **cee-map <CEE-map-id(1-4)>**

no cee-map <CEE-map-id(1-4)>

Parameter Description `<CEE-map-id(1-4)>` - Specify the index of CEE-Maps to configure.

Mode Global Configuration Mode

Example

```
SMIS# configure terminal
SMIS(config)# cee-map 1
SMIS(config-cee-map)# exit
SMIS(config)#
```

Related Command(s)

- `show cee-map` – List the defined CEE-Maps in the system.
- `group-bandwidth` – Allocate egress bandwidth for priority-groups.
- `group` – Add description text string to priority-groups.
- `pri2pg` – Define the mapping between traffic priorities and priority-groups.
- `priority` – Add description text string to traffic priorities.
- `pfc group` – Declare whether to enable the PFC feature for priority-groups.
- `pfc priority` – Declear whether to enable the PFC feature for traffic priorities.

group-bandwidth

Command Objective This command defines the egress bandwidth allocation for each priority-group in percentage.

No form of this command restore the default allocation.

Syntax **group-bandwidth <pg0%(0-100)> <pg1%(0-100)> <pg2%(0-100)> <pg3%(0-100)> <pg4%(0-100)> <pg5%(0-100)> <pg6%(0-100)> <pg7%(0-100)>**

no group-bandwidth

Parameter Description

- `<pg0%(0-100)>` - Egress bandwidth percentage for priority-group 0
- `<pg1%(0-100)>` - Egress bandwidth percentage for priority-group 1
- `<pg2%(0-100)>` - Egress bandwidth percentage for priority-group 2
- `<pg3%(0-100)>` - Egress bandwidth percentage for priority-group 3
- `<pg4%(0-100)>` - Egress bandwidth percentage for priority-group 4
- `<pg5%(0-100)>` - Egress bandwidth percentage for priority-group 5

- `<pg6%(0-100)>` - Egress bandwidth percentage for priority-group 6
- `<pg7%(0-100)>` - Egress bandwidth percentage for priority-group 7

Notes:

- The sum of priority-group 0-7 bandwidth must be 100.
- Zero percent can still get a very low bandwidth as CEE specification defined.

Mode CEE-Map Configuration

Example

```
SMIS(config)# cee-map 2
SMIS(config-cee-map)# group-bandwidth 25 25 10 10 20 5 5 0
SMIS(config-cee-map)# exit
SMIS(config)# show cee-map 2
CEE-Map 2
Ports :

Priority  Group  PFC  Description
-----------------------------------------------------
        0      0    No   LAN
        1      0    No
        2      0    No
        3      1   Yes   FCoE/FIP
        4      0    No
        5      0    No
        6      0    No
        7      0    No
Group  Bandwidht(%)  PFC  Description
-----------------------------------------------------------
     0            25    No   LAN
     1            25   Yes   SAN
     2            10    No
     3            10    No
     4            20    No
     5             5    No
     6             5    No
     7             0    No
     15          MAX    No
Application-Protocol-ID   Type       Pr tocol-ID     Priority
--------------------------------------------------------------------------------------------
                       1   ether-type 0x8906          3
                       2   ether-type 0x8914          3
                       3   tcp-udp    3260            4
```

Related Command(s) `cee-map` – Create or enter a CEE-Map to configure.

group

Command Objective This command adds descriptions to priority-groups.

The no form of this command restore the default allocation.

Syntax **group <id(0-7,15)> description {<string(63)>}**

no group <id(0-7,15)> description

Parameter Description

- `group <id(0-7,15)>` - Specify the priority-group ID
- `description {<string(63)>}` – Description string

Mode CEE-Map Configuration

Example

```
SMIS(config)# cee-map 2
SMIS(config-cee-map)# group 4 description "Internet traffic"
SMIS(config-cee-map)# exit
SMIS(config)# show cee-map 2
CEE-Map 2
Ports :
Priority  Group  PFC  Description
------------------------------------------------------------
       0      0   No  LAN
       1      0   No
       2      0   No
       3      1   Yes  FCoE/FIP
       4      0   No
       5      0   No
       6      0   No
       7      0   No
Group   Bandwidht(%)   PFC  Description
-------------------------------------------
    0           20    No  LAN
    1           80    Yes  SAN
    2            0    No
    3            0    No
    4            0    No  Internet traffic
    5            0    No
    6            0    No
    7            0    No
    15          MAX   No
Application-Protocol-ID   Type       Protocol-ID    Priority
--------------------------------------------------------------------------------------------------------
                     1   ether-type 0x8906         3
                     2   ether-type 0x8914         3
                     3   tcp-udp    3260           4
```

Related Command(s) `cee-map` – Create or enter a CEE-Map to configure.

pri2pg

Command Objective This command maps traffic priorities to priority-group.

No form of this command restore the default allocation.

Syntax **pri2pg <pri0-gid(0-7,15)> <pri1-gid(0-7,15)> <pri2-gid(0-7,15)> <pri3-gid(0-7,15)> <pri4-gid(0-7,15)> <pri5-gid(0-7,15)> <pri6-gid(0-7,15)> <pri7-gid(0-7,15)>**

no pri2pg [{priority <integer(0-7)>| all}]

Parameter Description

- <pri0-gid(0-7,15)>- The priority-group that traffic priority 0 belongs to
- <pri1-gid(0-7,15)>- The priority-group that traffic priority 1 belongs to
- <pri2-gid(0-7,15)>- The priority-group that traffic priority 2 belongs to
- <pri3-gid(0-7,15)>- The priority-group that traffic priority 3 belongs to
- <pri4-gid(0-7,15)> - The priority-group that traffic priority 4 belongs to
- <pri5-gid(0-7,15)>- The priority-group that traffic priority 5 belongs to
- <pri6-gid(0-7,15)>- The priority-group that traffic priority 6 belongs to
- <pri7-gid(0-7,15)>- The priority-group that traffic priority 7 belongs to
- [{priority <integer(0-7)>| all}] – Specify which traffic priorities to reset the mapping

Mode CEE-Map Configuration

Example

```
SMIS(config)# cee-map 2
SMIS(config-cee-map)# pri2pg 2 2 4 4 0 0 0 7
SMIS(config-cee-map)# exit
SMIS(config)# show cee-map 2
CEE-Map 2
Ports :
Priority  Group  PFC  Description
-----------------------------------------------------------------
       0      2   No  LAN
       1      2   No
       2      4   No
       3      4   Yes  FCoE/FIP
       4      0   No
       5      0   No
       6      0   No
       7      7   No
Group   Bandwidht(%)   PFC  Description
----------------------------------------------------------------
    0            20   No  LAN
    1            80   Yes  SAN
    2             0   No
    3             0   No
    4             0   No
    5             0   No
    6             0   No
    7              0    No
    15            MAX   No
 Application-Protocol-ID   Type       Protocol-ID     Priority
-----------------------------------------------------------------------------------------------------------
                        1   ether-type 0x8906         3
                        2   ether-type 0x8914         3
                        3   tcp-udp    3260           4
```

Related Command(s) `cee-map` – Create or enter a CEE-Map to configure.

priority

Command Objective This command adds descriptions to traffic priorities

No form of this command restores the default allocation.

Syntax **priority <pri(0-7)> description <string(63)>**

no priority <pri(0-7)> description

Parameter Description

- `priority <pri(0-7)>` - Specify the traffic priority
- `description <string(63)>` – Description string

Mode CEE-Map Configuration

Example

```
SMIS(config)# cee-map 2
SMIS(config-cee-map)# priority 0 description "LAN data"
SMIS(config-cee-map)# priority 1 description "LAN data higher priority"
SMIS(config-cee-map)# priority 2 description "Sensor data exchange"
SMIS(config-cee-map)# priority 3 description "FCoE SAN traffic"
SMIS(config-cee-map)# exit
SMIS(config)# show cee-map 2
CEE-Map 2
Ports :
Priority  Group  PFC  Description
-------------------------------------------------------
       0      0   No  LAN data
       1      0   No  LAN data higher priority
       2      0   No  Sensor data exchange
       3      1  Yes  FCoE SAN traffic
       4      0   No
       5      0   No
       6      0   No
       7      0   No
Group  Bandwidht(%)  PFC  Description
-------------------------------------------------------------
    0            20   No  LAN
    1            80  Yes  SAN
    2             0   No
    3             0    No
    4             0    No
    5             0    No
    6             0    No
    7             0    No
    15           MAX    No
-----
 Application-Protocol-ID   Type       Protocol-ID    Priority
-------------------------------------------------------------------------------------------------------------------------
                       1   ether-type 0x8906         3
                       2   ether-type 0x8914         3
                       3   tcp-udp    3260           4
```

Related Command(s) `cee-map` – Create or enter a CEE-Map to configure.

pfc group

Command Objective This command defines whether to enable the PFC feature for the specified priority-group.

Syntax **pfc group <id(0-7)> {enable|disable}**

Parameter Description

- `group <id(0-7)>` – Specify the priority-group
- `{enable|disable}` – Enable or disable the PFC feature, for all the members of the priority group

Mode CEE-Map Configuration

Example

```
SMIS(config)# cee-map 2
SMIS(config-cee-map)# pfc group 4 enable
SMIS(config-cee-map)# pfc group 5 enable
SMIS(config-cee-map)# pfc group 6 enable
SMIS(config-cee-map)# exit
SMIS(config)# show cee-map 2
CEE-Map 2
Ports :
Priority Group PFC  Description
-----------------------------------------------------------------------
       0       0    No   LAN
       1       0    No
       2       0    No
       3       1    Yes   FCoE/FIP
       4       0    No
       5       0    No
       6       0    No
       7       0    No
 Group   Bandwidht(%)   PFC   Description
---------------------------------------------------
    0             20    No   LAN
    1             80   Yes   SAN
    2              0    No
    3              0    No
    4              0   Yes
    5              0   Yes
    6              0   Yes
-----    7              0    No
    15            MAX   No
 Application-Protocol-ID   Type        Protocol-ID     Priority
---------------------------------------------------------------------------------------
                       1   ether-type  0x8906          3
                       2   ether-type  0x8914          3
                       3   tcp-udp     3260            4
```

Related Command(s) `cee-map` – Create or enter a CEE-Map to configure.

pfc priority

Command Objective This command defines whether to enable the PFC feature for the specified traffic priority.

Syntax **PFC priority <pri(0-7)> {enable|disable}**

Parameter Description

- `priority <pri(0-7)>` – Specify the traffic priority
- `{enable|disable}` – Enable or disable the PFC feature, for the traffic priority individually

Mode CEE-Map Configuration

Example

```
SMIS(config)# cee-map 2
SMIS(config-cee-map)# pfc priority 5 enable
SMIS(config-cee-map)# pfc priority 6 enable
SMIS(config-cee-map)# pfc priority 7 enable
SMIS(config-cee-map)# exit
SMIS(config)# show cee-map 2
CEE-Map 2
Ports :
Priority Group PFC  Description
--------------------------------------------------------------------
       0       0   No  LAN
       1       0   No
       2       0   No
       3       1   Yes  FCoE/FIP
       4       0   No
       5       0   Yes
       6       0   Yes
       7       0   Yes
 Group   Bandwidht(%)   PFC  Description
--------------------------------------------------
```

```
-----------------------------------------------------------------------
    0            20    No   LAN
    1            80    Yes   SAN
    2             0    No
    3             0    No
    4             0    No
    5             0    No
    6             0    No
    7             0    No
    15          MAX    No
 Application-Protocol-ID   Type       Protocol-ID    Priority
--------------------------------------------------------------------------------------------------------------
                      1    ether-type 0x8906         3
                      2    ether-type 0x8914         3
                      3    tcp-udp    3260           4
```

Related Command(s) `cee-map` – Create or enter a CEE-Map to configure.

cee

Command Objective This command associates the interface with a CEE-Map.

No form of this command removes the association.

Syntax **cee <cee-map-id(1-4))>**

no cee

Parameter Description `cee <cee-map-id(1-4))>` – Specifying the CEE-Map to associate

Mode Interface Configuration Mode

Example

```
SMIS(config)# interface ex 0/56
SMIS(config-if)# cee 1
SMIS(config-if)# exit
SMIS(config)#
```

Related Command(s)

- `dcbx cee` – Start DCBX on an interface.
- `lldp tlv-select dcbx-cee-pfc` – Configure the transmitting PFC TLV.
- `lldp tlv-select dcbx-cee-pg` – Configure the transmitting PG TLV.

dcbx cee

Command Objective This command starts DCBX on an interface, .

No form of this command stops DCBX.

Notes: Since DCBX required LLDP in operating, so make sure LLDP is enabled to advertise LLDPDUs.

Syntax **dcbx cee**

no dcbx cee

Parameter Description None

Mode Interface Configuration Mode

Example

```
SMIS(config)# interface extreme-ethernet 0/57
SMIS(config-if)# cee 1
SMIS(config-if)# dcbx cee
SMIS(config-if)# exit
SMIS(config)#
SMIS(config)# interface extreme-ethernet 0/58
SMIS(config-if)# no dcbx cee
SMIS(config-if)# no cee
SMIS(config-if)# exit
```

Related Command(s)

- `dcbx cee` – Start DCBX on an interface.
- `lldp tlv-select dcbx-cee-pfc` – Configure the transmitting PFC TLV.
- `lldp tlv-select dcbx-cee-pg` – Configure the transmitting PG TLV.

lldp tlv-select dcbx-cee-pfc

Command Objective Configure whether to advertise PFC feature sub-TLV in the CEE TLV, and set the values of Willing bit and Enabled bit.

The no form of this command restores the default settings.

Note: Since DCBX required LLDP in operating, so make sure LLDP is enabled to advertise LLDPDUs.

Syntax **lldp tlv-select dcbx-cee-pfc [advertise {on|off}] [willing {0|1}] [enable {0|1}]**

no lldp tlv-select dcbx-cee-pfc

Parameter Description

- `[advertise {on|off}]` – Switch on/off the PFC sub-TLV appending in the transmitting LLDPDU.
- `[willing {0|1}]` – The Willing bit value of the transmitting PFC sub-TLV.
- `[enable {0|1}]` – The Enabled bit value of the transmitting PFC sub-TLV.

Mode Interface Configuration Mode

Example

```
SMIS(config)# interface extreme-ethernet 0/57
SMIS(config-if)# lldp tlv-select dcbx-cee-pfc advertise on willing 0 enable 1
SMIS(config-if)# exit
```

Related Command(s)

- `dcbx cee` – Start DCBX on an interface.
- `lldp tlv-select dcbx-cee-pg` – Configure the transmitting PG TLV.

lldp tlv-select dcbx-cee-pg

Command Objective Configure whether to advertise PG feature sub-TLV in the CEE TLV, and set the values of Willing bit and Enabled bit.

No form of this command restores the default settings.

Note: Since DCBX required LLDP in operating, so make sure LLDP is enabled to advertise LLDPDUs.

Syntax **lldp tlv-select dcbx-cee-pg [advertise {on|off}] [willing {0|1}] [enable {0|1}]**

no lldp tlv-select dcbx-cee-pg

Parameter Description

- `[advertise {on|off}]` – Switch on/off the PG sub-TLV appending in the transmitting LLDPDU.
- `[willing {0|1}]` – The Willing bit value of the transmitting PFC sub-TLV.
- `[enable {0|1}]` – The Enabled bit value of the transmitting PFC sub-TLV.

Mode Interface Configuration Mode

Example

```
SMIS(config)# interface extreme-ethernet 0/57
SMIS(config-if)# lldp tlv-select dcbx-cee-pg advertise on willing 0 enable 1
SMIS(config-if)# exit
```

Related Command(s)

- `dcbx cee` – Start DCBX on an interface.
- `lldp tlv-select dcbx-cee-pfc` – Configure the transmitting PFC TLV.

30 OSPF

OSPF (Open Shortest Path First) protocol, is an Interior Gateway Protocol used to distribute routing information within a single Autonomous System. Routers use link-state algorithms to send routing information to all nodes in an inter-network by calculating the shortest path to each node based on topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations), which describes the state of its own links, and it also sends the complete routing structure (topography).

The advantage of shortest path first algorithms is that they result in smaller more frequent updates everywhere. They converge quickly, thus preventing such problems as routing loops and Count-to-Infinity (when routers continuously increment the hop count to a particular network). This makes for a stable network.

Before configuring OSPF, RRD must be enabled. This can be done by defining RRD_WANTED in LR/make.h in compilation. In addition, all OSPF interface related configurations, can be done only when the global OSPF is enabled.

The list of CLI commands for the configuration of OSPF is common to both Single Instance and Multiple Instance except for a difference in the prompt that appears for the Switch with Multiple Instance support.

The prompt for the Global Configuration Mode is,
Your Product(config)#

The parameters specific to Multiple Instance are stated so, against the respective parameter descriptions in this document.

The outputs of the Show commands differ for Single Instance and Multiple Instance. Hence both the outputs are documented while depicting the show command examples.
The list of CLI commands for the configuration of OSPF is as follows:

- router ospf
- router-id
- area – virtual-link
- area - stub
- area - nssa
- area – default cost
- area – stability interval
- area – translation-role
- area - range
- compatible rfc1583
- abr-type
- neighbor
- default-information originate always
- ASBR Router
- summary-address
- redistribute

- distribute-list route-map in
- redist-config
- capability opaque
- nsf ietf restart-support
- nsf ietf restart-interval
- nsf ietf helper-support
- nsf ietf helper gracetimelimit
- nsf ietf helper strict-lsa-checking
- nsf ietf grace lsa ack required
- nsf ietf grlsa retrans count
- nsf ietf restart-reason
- distance
- route-calculation staggering
- route-calculation staggering-interval
- network
- set nssa asbr-default-route translator
- passive-interface vlan
- passive-interface default
- ip ospf demand-circuit
- ip ospf retransmit-interval
- ip ospf transmit-delay
- ip ospf priority
- ip ospf hello-interval
- ip ospf dead-interval
- ip ospf cost
- ip ospf network
- ip ospf authentication-key
- ip ospf message-digest-key
- ip ospf authentication
- debug ip ospf
- show ip ospf
- show ip ospf – interface
- show ip ospf – neighbor
- show ip ospf – request-list
- show ip ospf – retransmission-list
- show ip ospf – virtual-links
- show ip ospf – border-routers
- show ip ospf – summary address
- show ip ospf – route
- show ip ospf – database
- show ip ospf – database summary
- show ip ospf redundancy
- ip ospf key start-accept

- ip ospf key start-generate
- ip ospf key stop-generate
- ip ospf key stop-accept
- timers spf
- area – virtual-link key start-accept
- area – virtual-link key start-generate
- area – virtual-link key stop-generate
- area – virtual-kink key stop-accept

router ospf

Command Objective This command enables OSPF routing process and enters into the OSPF Router Configuration Mode, which allows the user to execute all commands supporting this mode.

The no form of this command disables the OSPF Router Admin Status to terminate the OSPF process.

Syntax **router ospf [vrf <name>]**

no router ospf [vrf <name>]

Parameter Description `vrf <name>` - Enables OSPF for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size 32.

Mode Global Configuration Mode

Example

```
Your Product(config)# router ospf
Your Product (config-router)#
```

Related Command(s)

- `ip vrf` - Creates VRF instance
- `router-id` – Sets the router-id for the OSPF process
- `area – virtual-link` - Defines an OSPF virtual link.
- `area – stub` - Specifies an area as a stub area.
- `area – nssa` - Configures an area as a not-so-stub area (NSSA).
- `area – default cost` - Specifies a cost for the default summary route sent into a stub or NSSA.
- `area – stability-interval` - Configures the Stability interval for NSSA.
- `area – translation-role` - Configures the translation role for the NSSA,
- `area – range` - Consolidates and summarizes routes at an area boundary.
- `ip ospf demand-circuit` - Configures OSPF to treat the interface as an OSPF demand circuit.
- `ip ospf retransmit-interval` – Configures the time interval between link-state advertisement (LSA) retransmissions.
- `ip ospf transmit-delay` – Configures the estimated time required to transmit a link state update packet.
- `ip ospf priority` - Sets the router priority

- `ip ospf hello-interval` - Specifies the time interval between hello packets sent.
- `ip ospf dead-interval` - Sets the interval at which hello packets must not be seen before neighbors declare the router down.
- `ip ospf authentication-key` - Specifies a password to be used by neighboring routers that are using the OSPF simple password authentication.
- `ip ospf message-digest-key` - Enables OSPF MD5 authentication
- `ip ospf authentication` - Specifies the authentication type for an interface
- `default-information originate always` - Enables generation of a default external route into an OSPF routing domain
- `distance` - Enables the administrative distance
- `distribute-list route-map` – Enables inboumd filtering for routes.
- `neighbor` - Specifies a neighbor router and its priority
- `set nssa asbr-Default-route translator` - Enables setting of P bit in the default Type-7 LSA generated.
- `redist-config` - Configures the information to be applied to routes learnt from RTM.
- `redistribute` - Configures the protocol from which the routes have to be redistributed into OSPF.
- `passive-interface` - Suppresses routing updates on an interface.
- `abr-type` - Sets the Alternative ABR Type.
- `passive-interface default` - Suppresses routing updates on all interfaces.
- `passive-interface` - suppresses routing updates on an interface and makes the interface as passive
- `distribute-list route-map in` - Enables inbound filtering for routes
- `capability opaque` - Enables the capability of storing opaque LSAs
- `nsf ietf restart-support` - Enables the graceful restart support
- `nsf ietf restart-interval` - Configures the OSPF graceful restart timeout interval
- `nsf ietf helper-support` - Enables the helper support
- `nsf ietf helper gracetimelimit` - Configures the graceful restart interval limit in helper side
- `nsf ietf helper strict-lsa-checking` - Enables the strict LSA check option in helper
- `nsf ietf grace lsa ack required` - Enables Grace Ack Required state in restarter
- `nsf ietf grlsa retrains count` - Configures the maximum number of retransmissions for type for unacknowledged GraceLSA
- `nsf ietf restart-reason` - Configures the reason for graceful restart
- `distance` - Enables the administrative distance of the routing protocol and sets the administrative distance value
- `route-calculation staggering` - Enables OSPF route calculation staggering feature
- `route-calculation staggering-interval` - Configures the OSPF route calculation staggering interval
- `network` – Defines the interfaces on which OSPF runs and area ID for those interfaces
- `show ip ospf route` – Displays routes learnt by OSPF process
- `show ip ospf – database` - Displays OSPF Database summary for the LSA type.
- `timers spf` - Configures the delay time and the hold time between two consecutive SPF calculations
- `area -virtual link key start-accept` – Configuring the Start Accept Time for Cryptographic

Key

- `area -virtual link key start-generate` – Configuring Start Generate Time for Cryptographic Key
- `area -virtual link key stop-accept` – Configuring Stop Accept time for Cryptographic Key
- `area -virtual link key stop-generate` – Configuring Stop Generate Time for Cryptographic Key
- `enable bfd` – enables BFD feature in OSPF
- `disable bfd` – Disables BFD feature in OSPF
- `bfd` – enables BFD monitoring on all or specifc OSPF interfaces
- `show ip ospf` – Displays general information about OSPF routing process

router-id

Command Objective This command sets the router-id for the OSPF process. The router ID is set to an IP address of a loopback interface if it is configured. An arbitrary value for the ip-address for each router can be configured; however, each router ID must be unique. To ensure uniqueness, the router-id must match with one of the router's IP interface addresses.

The no form of this command resets the configured router-id and dynamically select least interface ip as router-id for OSPF process

Syntax **router-id <router ip address>**

no router-id

Mode OSPF Router Configuration Mode

Example Your Product(config-router)# router-id 10.0.0.1

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `summary-address` – Creates aggregate addresses for OSPF
- `show ip ospf` – request-list - Displays OSPF Link state request list information
- `show ip ospf - retransmission-list` - Displays list of all OSPF Link state retransmission list information
- `show ip ospf` - Displays OSPF Link state request list
- `show ip ospf` - database - Displays OSPF LSA database summary.

area - virtual-link

Command Objective This command defines an OSPF virtual link and its related parameter. In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link. Hello-interval and dead-interval values must be the same for all routers and access servers on a specific network.

The no form of removes an OSPF virtual link.

Syntax **area <area-id> virtual-link <router-id> [authentication { simple |message-digest | sha-1 | sha-224 | sha-256 | sha384 | sha-512 | null}] [hello-interval <value (1-65535)>] [retransmit-interval <value (1-3600)>] [transmit-delay <value (1-3600)>] [dead-interval <value>] [{authentication-key <key (8)> | message-digest-key <Key-id (0-255)> {md5 | sha-1 | sha-224 | sha-256 | sha-384 | sha-512} <key (16)>}]**

no area <area-id> virtual-link <router-id> [authentication] [hello-interval] [retransmit-interval] [transmit-delay] [dead-interval] [{authentication-key | message-digest-key <Key-id (0-255)>}]

Parameter Description

- `<area-id>` - Configures the area ID assigned to the transit area for the virtual link. The Transit Area that the Virtual Link traverses. It is specified as an IP address This can be either a decimal value or a valid IP address.
- `<router-id>` - Configures the router ID of the virtual neighbor.
- `authentication` - Configures the authentication type. The list contains:
  - `Simple` – Sets the authentication type as simple password authentication mechanism.
  - `message-digest` – Sets the authentication type as message digest authentication mechanism.
  - `sha-1` - Sets the authentication type as Secure Hash Algorithm 1(SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes.
  - `sha-224` - Sets the authentication type as Secure Hash Algorithm 224(SHA224) authentication. SHA224 generates Authentication digest of length 28 bytes.
  - `sha-256` - Sets the authentication type as Secure Hash Algorithm 256(SHA256) authentication. SHA256 generates Authentication digest of length 32 bytes.
  - `sha-384` - Sets the authentication type as Secure Hash Algorithm 384(SHA384) authentication. SHA384 generates Authentication digest of length 48 bytes.
  - `sha-512` - Sets the authentication type as Secure Hash Algorithm 512(SHA512) authentication. SHA512 generates Authentication digest of length 64 bytes.
  - `null` – Sets the no password authentication.
- `hello-interval<value (1-65535)>` - Sets the interval between hello packets that the software sends on the OSPF virtual link interface. This value ranges between 1 and 65535 in seconds.
- `retransmit-interval <value (1-3600)>` - Sets the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPF virtual link interface. This value ranges between 1 and 3600 in seconds.
- `transmit-delay <value (1-3600)>` - Sets the time in which the router will stop using this key for packets generation. Estimated time required to send a link-state update packet on the interface. Integer value that must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. This value ranges between 1 and 3600 in seconds.
- `dead-interval <value>` - Sets the interval at which hello packets must not be seen before its neighbors declare the router down. As with the hello interval, this value must be the same for all

routers and access servers attached to a common network. This value ranges between 1 and 65535 seconds.

- `authentication-key <key (8)>` - Identifies the secret key used to create the message digest appended to the OSPF packet Password to be used by neighboring routers. This string acts as a key that will allow the authentication procedure to generate or verify the authentication field in the OSPF header. This is a sting with maximum string size 8.
- `message-digest-key <Key-id (0-255)>` - Enables Message Digest 5 (MD5) authentication on the area specified by the area-id. This value ranges between 0 and 255.
- `md5` - Configures the authentication type as Message Digest 5 (MD5) authentication.
- `sha-1` - Sets the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes.
- `sha-224` – Sets the authentication type as Secure Hash Algorithm 224 (SHA224) authentication. SHA224 generates Authentication digest of length 28 bytes.
- `sha-256` - Sets the authentication type as Secure Hash Algorithm 256 (SHA256) authentication. SHA256 generates Authentication digest of length 32 bytes.
- `sha-384` - Sets the authentication type as Secure Hash Algorithm 384 (SHA384) authentication. SHA384 generates Authentication digest of length 48 bytes.
- `sha-512` - Sets the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. SHA512 generates Authentication digest of length 64 bytes.
- `<key (16)>` - Configures the cryptographic key value which is used used to create the message digest appended to the OSPF packet. All neighboring routers on the same network must have the same key identifier and key to route OSPF traffic. This is a sting with maximum string size 16.

Mode Router Configuration Mode

- Authentication – null
- hello-interval – 10 seconds
- retransmit-interval – 5 seconds
- transmit-delay – 1 seconds
- dead-interval – 40 seconds

Note: This command executes only if area is defined using the network command

Example

```
Your Product(config-router)# area 12.0.0.0 virtual-link 10.0.0.0
authentication simple hello-interval 65 retransmit-interval 654 dead-
interval 200 message-digest-key 20 sha-512 key11
```

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `ip ospf authentication` – Specifies the authentication type for an interface
- `network` – Defines the interfaces on which OSPF runs and area ID for those interfaces.
- `show ip ospf` – Displays general information about OSPF routing process
- `show ip ospf` – virtual –links - Displays parameters and the current state of OSPF virtual links
- `area -virtual link key start-accept` – Configuring the Start Accept Time for Cryptographic Key

- `area -virtual link key start-generate` – Configuring Start Generate Time for Cryptographic Key
- `area -virtual link key start-generate` – Configuring Start Generate Time for Cryptographic Key
- `area -virtual link key stop-accept` – Configuring Stop Accept Time for Cryptographic Key
- `area -virtual link key stop-generate` – Configuring Stop Generate Time for Cryptographic Key

area - stub

Command Objective This command specifies an area as a stub area and other parameters related to that area. This command is configured on all routers and access servers in the stub area.

The no form of the command removes an area or converts stub/nssa to normal area.

Syntax **area <area-id> stub [no-summary]**

no area <area-id> [{ stub [no-summary] | nssa [no-redistribution] [Default-information-originate [metric<value>] [metric-type <Type(1-3)>]][no-summary]}]

Parameter Description

- `<area-id>` - Configures the identifier of the area associated with the OSPF address range for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address
- `no-summary` - Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area by neither originating nor propagating summary LSA into the stub area
- `nssa` - Configures the area as Not-So-Stubby Area (NSSA).
    - no-redistribution -Disables redistribution of routes from the given protocol into OSPF.
- `Default-information originate` - Configures default route into OSPF.
    - `metric <value>` - Configures metric related configurations applied to the route before it is advertised into the OSPF domain. This value ranges between 0 and 16777215.
    - `metric-type <Type(1-3)>` - Configures the metric type applied to the route before it is advertised into the OSPF domain. This value ranges between 1 and 3.
- `no-summary`- Allows an area to be a not-so-stubby area but not have summary routes injected into it.

Mode OSPF Router Configuration Mode

Default

- Metric – 10
- Metric Type - 2

Example

```
Your Product(config-router)# area 10.0.0.1 stub
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `show ip ospf` – Displays general information about OSPF routing process

area - nssa

Command Objective This command configures a particular area as not-so-stubby area (NSSA).

The no form of the command sets the priority for the virtual router to its default value.

Syntax **area <area-id> nssa [{ no-summary | default-information-originate [metric <value (0-16777215)>] [metric-type <Type(1-3)>] [tos <tos value (0-30)>] [no-redistribution] }]**

no area <area-id> [{ stub [no-summary] | nssa [no-redistribution] [Default-information-originate [metric<value>] [metric-type <Type(1-3)>]][no-summary]}]

Parameter Description

- `<area-id>` - Configures the identifier of the area associated with the OSPF address range for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address.
- `no-summary` - Allows an area to be a not-so-stubby area but not have summary routes injected into it.
- `Default-information-originate` - Configures the default route into OSPF and used to generate a Type 7 default into the NSSA area.
  - `metric <value (0-16777215)>`- The Metric value applied to the route before it is advertised into the OSPF domain. This value ranges between 0 and 16777215.
  - `metric-type <Type(1-3)>` - The Metric Type applied to the route before it is advertised into the OSPF domain. This value ranges between 1 and 3.
  - `tos <tos value (0-30)>` - Type of Service of the route being configured. This value ranges between 0 and 30. It can be configured only if the code is compiled with TOS Support
  - `no-redistribution` - Disables redistribution of routes from the given protocol into OSPF.

Mode Router Configuration Mode

Notes:

- `The no area <area-id> [{ stub | nssa }]` command removes an area or converts stub/nssa to normal area.
- The backbone area cannot be set as Stub or NSSA

Default

- metric -10
- metric-type - 1
- tos - 0

Example `Your Product(config-vrrp-if)# area 10.0.0.1 nssa`

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `area - default cost` - Specifies a cost for the default summary route
- `area - stability interval` - Configures the Stability interval for NSSA
- `area - range` – Consolidates and summarizes routes at an area boundary
- `show ip ospf` - Displays general information about the OSPF routing process.
- `summary-address` - Creates aggregate addresses for OSPF.

area - default cost

Command Objective This command specifies a cost for the default summary route sent into a stub or NSSA. This command is used only on an Area Border Router (ABR) attached to a stub or NSSA. This command provides the metric for the summary default route generated by the ABR into the stub area.

The no form of the command removes the assigned default route cost.

Syntax **area <area-id> default-cost <cost> [tos <tos value(0-30)>] no**

no area <area-id> default-cost [tos <tos value (0-30)>]

Parameter Description

- `<area-id>` - Configures the identifier for the stub or NSSA. The identifier can be specified as either a decimal value or as an IP address.
- `Default-cost<cost>` - Configures the cost for the default summary route used for a stub or NSSA. A default cost can be defined only for a valid area. This value ranges between 0 and 16777215.
- `tos<tos value(0-30)>` - Configures the Type of Service of the route being configured. The value ranges between 0 and 30. It can be configured only if the code is compiled with TOS Support

Mode OSPF Router Configuration Mode

Default

- default-cost - 1
- tos - 0

Note: This command executes only if NSSA is configured.

Example `Your Product(config-router)# area 10.0.0.1 default-cost 5`

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `area- nssa` - Configures an area as a NSSA and other parameters related to that area.
- `ip ospf cost` – Specifies the cost of sending a packet on an interface
- `ip ospf authentication` – Specifies the authentication type for an interface

area - stability interval

Command Objective This command configures the Stability interval for NSSA where the Information describing the configured parameters and cumulative statistics of one of the router's attached areas.

The no form of the command configures default Stability interval for NSSA.

Syntax **area <area-id> stability-interval <Interval-Value (0 - 0x7fffffff)>**

no area <area-id> stability-interval

Parameter Description

- `<area-id>` - Configures the area id associated with the OSPF address range(ipv4 address). Area ID 0.0.0.0 is used for the OSPF backbone.
- `<Interval-Value (0 - 0x7fffffff)>` - Configures the time interval after an elected translator determines its services are no longer required, that it must continue to perform its translation duties. The interval value ranges between 0-0x7fffffff in seconds.The OSPF Sequence Number is a 32 bit signed integer. It starts with the value '80000001'h, -- or - '7FFFFFFF', and increments until '7FFFFFFF'h. Thus, a typical sequence number will be very negative

Mode OSPF Router Configuration Mode

Default 40 seconds

Note: This command executes only if NSSA is configured.

Example

```
Your Product(config-router)# area 10.0.0.1 stability-interval 10000
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `area- nssa` - Configures an area as a NSSA and other parameters related to that area.

area - translation-role

Command Objective This command configures the translation role for the NSSA.

The no form of the command configures the default translation role for the NSSA.

Syntax **area <area-id> translation-role { always | candidate }**

area <area-id> translation-role

Parameter Description

- `<area-id>` - Configures the area id associated with the OSPF address range. It is specified as an IP address
- `translation-role` -Configures Aan NSSA Border router's ability to perform NSSA Translation of Type-7 LSAs to Type-5 LSAs.The options are :
  - `always`– Sets translator role where the Type-7 LSAs are always translated into Type-5 LSAs

    Type-5 LSAs- Originated by AS (Autonomous system) boundary routers, and flooded through-out the AS. Each AS-external-LSA describes a route to a destination in another Autonomous System. default routes for the AS can also be described by AS-external-LSAs
  - `candidate` – Sets translator role where an NSSA border router participates in the translator election process.

Mode OSPF Router Configuration Mode

Default Candidate

Example

```
Your Product(config-router)# area 10.0.0.1 translation-role always
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `area- nssa` - Configures an area as a NSSA and other parameters related to that area.

area - range

Command Objective This command consolidates and summarizes routes at an area boundary which is used only with Area Border Routers (ABRs). The result is that a single summary route is advertised to other areas by the ABR.

The no form of the command deletes the Summary Address.

Syntax **area <AreaId> range <Network> <Mask> {summary | Type7} [{advertise | not-advertise}] [tag <value>]**

no area <AreaId> range <Network> <Mask> [type7] [{advertise | not-advertise}] [tag <tag-value>] [cost <value>]

Notes:

- If the no command is executed without the optional parameter Type7, it deletes the Summary LSA.

- Advertise, not-advertise, tag-value and cost value is not supported to delete an area range in ospf.

Parameter Description

- `<AreaId>` - Configures the area associated with the OSPF address range and the identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IP address
- `<Network>` - Configures the IP address of the network indicated by the range.
- `<Mask>` - Configures the subnet mask that pertains to the range. The mask indicates the range of addresses being described by the particular route. For example, a summary-LSA for the destination 128.185.0.0 with a mask of 0xffff0000 actually is describing a single route to the collection of destinations 128.185.0.0 - 128.185.255.255.
- `summary` - Sets the LSA type as summary LSA.
- `Type7` - Sets the LSA type as Type-7 LSA.
- `advertise` - Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA). When associated area Id is 0.0.0.0, aggregated Type-5 are generated. For associated other than 0.0.0.0 aggregated Type-7 is generated in NSSA x.x.x.x

  Note: This parameter is currently not supported in the no form of the command.

- `not-advertise` - Sets the address range status to Not Advertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks When associated area Id is 0.0.0.0, Type-5 is not generated for the specified range, while aggregated Type-7 are generated in all attached NSSA. For associated are Id x.x.x.x other than 0.0.0.0, Type-7 are not generated in NSSA x.x.x.x for the specified range.

  Note: This parameter is currently not supported in the no form of the command.

- `tag <tag-value>` - Configures the Tag Type which describes whether Tags will be generated automatically or manually configured. This value ranges between 0 and 2147483647.

  Note: This parameter is currently not supported in the no form of the command.

- cost <value> - Configures the route path cost.

  Note: This parameter is currently not supported in the no form of the command.

Mode Router Configuration Mode

Default tag - 2

Note: This command executes only if a particular area is configured as NSSA.

Example

```
Your Product(config-router)# area 10.0.0.1 range 10.0.0.0 255.0.0.0 summary
advertise tag 10
```

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `area – nssa` - Configures a particular area as NSSA.
- `summary-address` – Creates aggregate addresses for OSPF
- `show ip ospf - summary address` – Displays OSPF Summary-address redistribution Information

compatible rfc1583

Command Objective This command sets OSPF compatibility list compatible with RFC 1583 and controls the preference rules, when choosing among multiple AS external LSAs advertising the same destination. When compatible is set to enable, the preference rules remain those specified by RFC1583. When compatible is set to disabled the preference rules are those stated in RFC2178.

The no form of the command disables RFC 1583 compatibility.

Syntax **compatible rfc1583**

no compatible rfc1583

Mode OSPF Router Configuration Mode

Default OSPF is Compatible

Example Your Product(config-router)# compatible rfc1583

Related Command(s) `router ospf` – Enables OSPF routing process

abr-type

Command Objective This command sets the Alternative ABR Type.

The no form of the command resets the configured Alternative ABR Type.

Syntax **abr-type { standard | cisco | ibm }**

no abr-type

Parameter Description

- `standard` - Configures the Standard ABR type as defined in RFC 2328
- `cisco` - Configures the CISCO ABR type as defined in RFC 3509
- `ibm` - Configures the IBM ABR type as defined in RFC 3509

Mode OSPF Router Configuration Mode

Default Standard

Notes:

- RFC 2328 **–** OSPF Version 2.
- RFC-3509 -- Alternative Implementations of OSPF Area Border Routers.

Example

```
Your Product(config-router)# abr-type standard
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `show ip ospf` – Displays general information about the OSPF routing process.

neighbor

Command Objective This command specifies a neighbor router and its priority. This command configures the Router ID of the. OSPF routers interconnecting to nonbroadcast networks.

The no form of this command removes the neighbor and resets the neighbor priority to its default value.

Syntax **neighbor <neighbor-id> [priority <priority value (0-255)>] [poll-interval seconds] [cost number] [database-filter all]**

no neighbor <neighbor-id> [priority] [poll-interval seconds] [cost number] [database-filter all out]

Parameter Description

- `<neighbor-id>` - Configures the Neighbor router ID based on which the priority of the neighbor is defined
- `priority <priority value (0-255)>` - Indicates a number value that specifies the router priority and the priority of the nonbroadcast neighbor router associated with the specified IP address. The router with the highest priority becomes the designated router. This value ranges between 0 and 255.The value 0 signifies that the neighbor is not eligible to become the designated router on this particular network.
- `poll-interval seconds` - Configures the poll interval between the Hello packets sent to an inactive non-broadcast multi-access neighbor.
- `cost number` - Configure route path cost value.
- `database-filter all` - Configures database filter.

Mode OSPF Router Configuration Mode

Default priority - 1

Example

```
Your Product(config-router)# neighbor 20.0.0.1 priority 25
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.

- `ip ospf priority` – Sets the router priority
- `ip ospf network` – Configures the OSPF network type to a type other than the default for a given media
- `show ip ospf neighbor` - Displays OSPF neighbor information list

default-information originate always

Command Objective This command enables generation of a default external route into an OSPF routing domain and other parameters related to that area.

The no form of the command disables generation of a default external route into an OSPF routing domain.

Syntax **default-information originate always [metric <metric-value (0-0xffffff)>][metric-type <type (1-2)>]**

no default-information originate always [metric <metric-value (0-0xffffff)>] [metric-type <type (1-2)>]

Parameter Description

- always - Advertises the default route always regardless of whether the software has a default route
- metric <metric-value (0-0xffffff)> - Sets the Metric value applied to the route before it is advertised into the OSPF Domain Metric used for generating the default route. If you omit a value and do not specify a value using the default-metric router configuration command, the default metric value is 1. The value used is specific to the protocol.
- metric-type <type (1-2)> - Sets the Metric Type applied to the route before it is advertised into the OSPF Domain External link type associated with the default route advertised into the OSPF routing domain. It can be one of the following values:
  1. Sets Type 1 external route
  2. Sets Type 2 external route

Mode OSPF Router Configuration Mode

Default

- metric - 10
- metric-type - 2

Example

```
Your Product(config-router)# default-information originate always metric 1
metric-type 1
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `redistribute` – Configures the protocol from which the routes have to be redistributed into OSPF

ASBR Router

Command Objective This command specifies this router as ASBR. Routers that act as gateways (redistribution) between OSPF and other routing protocols (IGRP, EIGRP, RIP, BGP, Static) or other instances of the OSPF routing process are called autonomous system boundary router (ASBR).

The no form of the command disables this router as ASBR.

Syntax **ASBR Router**

no ASBR Router

Parameter Description

- `always` - Advertises the default route always regardless of whether the software has a default route
- `metric <metric-value (0-0xffffff)>` - Sets the Metric value applied to the route before it is advertised into the OSPF Domain Metric used for generating the default route. If you omit a value and do not specify a value using the default-metric router configuration command, the default metric value is 1. The value used is specific to the protocol.
- `metric-type <type (1-2)>` - Sets the Metric Type applied to the route before it is advertised into the OSPF Domain External link type associated with the default route advertised into the OSPF routing domain. It can be one of the following values:
  1. Sets Type 1 external route
  2. Sets Type 2 external route

Mode OSPF Router Configuration Mode

Example `Your Product(config-router)# ASBR Router`

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `redistribute` – Configures the protocol from which the routes have to be redistributed into OSPF
- `redist-config` - Configures the information to be applied to routes learnt from RTM.
- `set nssa asbr-default-route translator` – Enables/disables setting of P bit in the default Type-7 LSA generated by NSSA internal ASBR
- `show ip ospf` – Displays general information about the OSPF routing process

summary-address

Command Objective This command creates aggregate addresses for OSPF and helps in reducing the size of the routing table.

The no form of the command deletes the External Summary Address.

Syntax **summary-address <Network> <Mask> <AreaId> [{allowAll | denyAll | advertise | not-advertise}] [Translation {enabled | disabled}][tag tag-value]**

no summary-address <Network> <Mask> <AreaId> [not-advertise] [tag tag-value]

Parameter Description

- `<Network>` - Configures the IP address of the Net indicated by the range.
- `<Mask>` - Configures the subnet mask that pertains to the range
- `<AreaId>` - Configures the area associated with the OSPF address range and the identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IP address.
- `allowAll` - Configures allowAll option and sets associated areaId as which generates the aggregated Type-5 for the specified range. In addition aggregated Type-7 are generated in all attached NSSA, for the specified rangeThis parameter is valid only for areaId 0.0.0.0.
- `denyAll` - Configures denyAll in which neither Type-5 nor Type-7 will be generated for the specified range. This parameter is valid only for areaId
- `advertise` - Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA). When associated area Id is 0.0.0.0, aggregated Type-5 are generated. Otherwise if associated areaId is x.x.x.x (other than 0.0.0.0) aggregated Type-7 is generated in NSSA x.x.x.x.
- `not-advertise` - Sets the address range status to NotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks When associated area Id is 0.0.0.0, Type-5 is not generated for the specified range, while aggregated Type-7 are generated in all attached NSSA. While if associated area Id is x.x.x.x(other than 0.0.0.0), Type-7 are not generated in NSSA x.x.x.x for the specified range. This parameter is currently not supported in the no form of the command.
- `Translation` - Indicates how an NSSA Border router is performing NSSA translation of Type-7 to into Type-5 LSAs.

  1. enabled **–** Sets P Bit in the generated Type-7 LSA.

  2. disabled - Clears P Bit in the generated Type-7 LSA.
- `tag tag-value` - Configures the tag option for OSPF.This parameter is currently not supported.

Mode OSPF Router Configuration Mode

Default

- summary-address – advertise
- translation - enabled

Note: This command executes only if NSSA is configured.

Example

```
Your Product(config-router)# summary-address 10.0.0.6 255.0.0.0 10.0.0.0
Translation enabled
```

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `area - nssa` - Configures a particular area as not-so-stubby area (NSSA).

- `area - range` – Consolidates and summarizes routes at an area boundary
- `show ip ospf` - `summary address` – Displays OSPF Summary-address redistribution Information
- `show ip ospf` - `database summary` – Displays OSPF LSA Database summary

redistribute

Command Objective This command configures the protocol from which the routes have to be redistributed into OSPF and advertises the routes learned by other protocols.

The no form of the command disables redistribution of routes from the given protocol.

Syntax **redistribute {static | connected | rip | bgp | all} [route-map <name(1-20)>] [metric <mertic_value(0-16777214)>] [metric-type {1-2}]**

no redistribute {static | connected | rip | bgp | all} [route-map <name(1-20)>] [metric]

Parameter Description

- static - Redistributes routes, configured statically, to the OSPF routing protocol.
- connected - Redistributes directly connected network routes, to the OSPF routing protocol.
- rip - Redistributes routes, that are learnt by the RIP process, to the OSPF routing protocol.
- bgp - Redistributes routes, that are learnt by the BGP process, to the OSPF routing protocol.
- all - Redistributes all routes to the OSPF routing protocol.
- route-map <name(1-20)> - Identifies the specified route-map in the list of route-maps. This is a string with maximum string size 20.
- metric <mertic_value(0-16777214)> - Configures the metric values for the routes to be redistributed into ospf. This value ranges between 0 and 16777214.
- metric-type {1-2} - Configures the metric type applied to the routes to be redistributed. This value ranges between 1 and 2.

Mode OSPF Router Configuration Mode

Default

- metric - 10
- metric-type - 2

Example

```
Your Product(config-router)# redistribute static
```

Related Command(s) `router ospf` – Enables OSPF routing process.

distribute-list route-map in

Command Objective This command enables inbound filtering for routes and defines the conditions for distributing the routes from one routing protocol to another.

The no form of the command disables inbound filtering for the routes.

Syntax **distribute-list route-map <name(1-20)> in**

no distribute-list route-map <name(1-20)> in

Parameter Description `<name(1-20)>` - Configures the name of the Route Map for which filtering should be enabled. Only one route map can be set for inbound routes. Another route map can be assigned, only if the already associated route map is disassociated. This value is a string with maximum string size 20.

Mode OSPF Router Configuration Mode

Default

- metric - 10
- metric-type - 2

Example

```
Your Product(config-router)# distribute-list route-map rmap-test in
```

Related Command(s) `router ospf` – Enables OSPF routing process.

redist-config

Command Objective This command configures the information to be applied to routes learnt from RTM.

The no form of the command deletes the information applied to routes learnt from RTM.

Syntax **redist-config <Network> <Mask> [metric-value <metric (1 - 16777215)>] [metric-type {asExttype1 | asExttype2}] [tag <tag-value>}**

no redist-config <Network> <Mask>

Parameter Description

- `<Network>` - Confgures the IP Address of the Destination route
- `<Mask>` - Configures the Mask of the Destination route
- `metric-value <metric (1 - 16777215)>` - Configures the Metric value applied to the route before it is advertised into the OSPF Domain. This value ranges between 1 and 16777215.
- `metric-type` - Configures the Metric Type applied to the route before it is advertised into the OSPF Domain. The list options are:
    - `asExttype1` – Sets the metric type as AS external type 1.
    - `asExttype2` – Sets the metric type as AS external type 2.
- `Tag <tag-value>` - Configures theTag Type describes whether Tags will be automatically generated or will be manually configured. This value ranges between 0 and 4294967295. This is not used by OSPF protocol itself. It may be used to communicate information between AS boundary routers. The precise nature of this information is outside the scope of OSPF. If tags are manually configured, the futospfRRDRouteTag MIB has to be set with the Tag value needed. To execute this command with

the tag option, the router must to set as ASBR

Mode OSPF Router Configuration Mode

Default

- metric - 10
- metric-type – asExttype2
- tag – manual

Note: This command executes only if the router is set as ASBR

Example

```
Your Product(config-router)# redist-config 10.0.0.0 255.0.0.0 metric-value
100 metric-type asExttype1
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `ASBR router` – Sets the router as ASBR
- `redistribute` – Configures the protocol from which the routes have to be redistributed into OSPF

capability opaque

Command Objective This command enables the capability of storing opaque LSAs.

The no form of the command disables the opaque capability.

Syntax **capability opaque**

no capability opaque

Mode OSPF Router Configuration Mode

Default Opaque capability is disabled.

Example Your Product(config-router)# capability opaque

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `nsf ietf restart-support` - Enables the graceful restart support

nsf ietf restart-support

Command Objective This command enables the graceful restart support in OSPF router. Graceful restart support is provided for both unplanned and planned restart, if the command is executed without any option. The graceful restart mechanism allows forwarding of data packets to continue along known routes, while the routing protocol information is being restored following a processor switch over. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent.

The no form of the command disables the graceful restart support.

Syntax **nsf ietf restart-support [plannedOnly]**

no nsf ietf restart-support

Parameter Description `plannedOnly`- Configures planned only graceful restart mechanism in the OSPF router.

Mode OSPF Router Configuration Mode

Default

Graceful restart support is disabled.

Note: This command executes only if the

- OSPF is enabled
- Opaque functionality is enabled.

Example

```
Your Product(config-router)# nsf ietf restart-support
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `capability opaque` - Enables the capability of storing opaque LSAs
- `show ip ospf` – Displays general information about OSPF routing process

nsf ietf restart-interval

Command Objective This command configures the OSPF graceful restart timeout interval. This value specifies the graceful restart interval, in seconds, during which the restarting router has to reacquire OSPF neighbors that are fully operational prior to the graceful restart. The value ranges between 1 and 1800 seconds. The value is provided as an intimation of the grace period to all neighbors. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent.

The no form of the command resets the interval to default value.

Syntax **nsf ietf restart-interval <grace period(1-1800)>**

no nsf ietf restart-interval

Mode OSPF Router Configuration Mode

Default 120 seconds

Example Your Product(config-router)# nsf ietf restart-interval 200

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `show ip ospf` – Displays general information about OSPF routing process.

nsf ietf helper-support

Command Objective This command enables the helper support. The helper support is enabled for all the options, if the command is executed without any option. The helper support can be enabled for more than one option, one after the other. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent.

The no form of the command disables the helper support. The helper support is disabled for all the options, if the command is executed without any option.

Syntax **nsf ietf helper-support [{unknown | softwareRestart | swReloadUpgrade | switchToRedundant}]**

no nsf ietf helper-support [{unknown | softwareRestart | swReloadUpgrade | switchToRedundant}]

Parameter Description

- `unknown` - Configures helper support for restarting of system due to unplanned events (such as restarting after a crash).
- `softwareRestart` - Configures helper support for restarting of system due to restart of software.
- `swReloadUpgrade` - Configures helper support for restarting of system due to reload or upgrade of software.
- `switchToRedundant` - Configures helper support for restarting of system due to switchover to a redundant support processor.

Mode OSPF Router Configuration Mode

Default Helper support is enabled.

Note: This command executes only if OSPF routing process is enabled

Example

```
Your Product(config-router)# nsf ietf helper-support switchToRedundant
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `nsf ietf helper gracetimelimit` - Configures the graceful restart interval limit in helper side
- `nsf ietf helper strict-lsa-checking` - Enables the strict LSA check option in helper
- `show ip ospf` – Displays general information about OSPF routing process

nsf ietf helper gracetimelimit

Command Objective This command configures the grace period till which the OSPF router acts as Helper. During this period, the router advertises that the restarting router is active and is in FULL state. The value ranges between 0 and 1800 seconds. The value is provided as an intimation of the restart period to the neighbors that do not support graceful restart or that are connected using multipoint interfaces.

The no form of the command disables the graceful restart support.

Syntax **nsf ietf helper gracetimelimit <gracelimit period(0-1800)>**

Mode OSPF Router Configuration Mode

Default 0

Note: This command executes only if

- OSPF router is enabled
- Helper Mode is enabled.

Example

```
Your Product(config-router)# nsf ietf helper gracetimelimit 100
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `nsf ietf helper-support` - Enables the helper support
- `show ip ospf` – Displays general information about OSPF routing process

nsf ietf helper strict-lsa-checking

Command Objective This command enables the strict LSA check option in helper. The strict LSA check option allows the helper to terminate the graceful restart, once a changed LSA that causes flooding during the restart process is detected. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent.

The no form of the command disables the strict LSA check option in helper.

Syntax **nsf ietf helper strict-lsa-checking**

no nsf ietf helper strict-lsa-checking

Mode OSPF Router Configuration Mode

Default Strict LSA check option is disabled in helper.

Note: This command executes only if

- OSPF router is enabled
- Helper Mode is enabled.

Example `Your Product(config-router)# nsf ietf helper strict-lsa-checking`

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `nsf ietf helper-support` - Enables the helper support
- `show ip ospf` – Displays general information about OSPF routing process

nsf ietf grace lsa ack required

Command Objective This command enables Grace Ack Required state in restarter. The GraceLSAs sent by the router are expected to be acknowledged by peers, if the Grace Ack Required state is enabled. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent

The no form of the command disables the graceful restart support.

Syntax **nsf ietf grace lsa ack require**

no nsf ietf grace lsa ack required

Mode OSPF Router Configuration Mode

Default Grace Ack Required state is enabled in restarter.

Note: This command executes only if OSPF router is enabled.

Example `Your Product(config-router)# nsf ietf grace lsa ack required`

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `show ip ospf` – Displays general information about OSPF routing process

nsf ietf grlsa retrans count

Command Objective This command configures the maximum number of retransmissions for unacknowledged GraceLSA. This value ranges between 0 and 180.

The no form of the command disables the strict LSA check option in helper.

Syntax **nsf ietf grlsa retrans count <grlsacout (0-180)>**

Mode OSPF Router Configuration Mode

Default 2

Note: This command executes only if OSPF router is enabled.

Example `Your Product(config-router)# nsf ietf grlsa retrans count 100`

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `show ip ospf` – Displays general information about OSPF routing process

nsf ietf restart-reason

Command Objective This command configures the reason for graceful restart in the OSPF router. The reason for restart can be software upgrade, scheduled restart or switch to redundant router. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent.

Syntax **nsf ietf restart-reason [{unknown | softwareRestart | swReloadUpgrade | switchToRedundant}]**

Parameter Description

- `unknown` - Configures the system to restart due to unplanned events (such as restarting after a crash).
- `softwareRestart` - Configures the system to restart due to software restart.
- `swReloadUpgrade` - Configures the system to restart due to reloading / upgrading of software.
- `switchToRedundant` - Configures the system to restart due to switchover to a redundant support processor.

Mode OSPF Router Configuration Mode

Default Unknown

Note: This command executes only if OSPF router is enabled

Example `Your Product(config-router)# nsf ietf restart-reason softwareRestart`

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `show ip ospf` – Displays general information about OSPF routing process

distance

Command Objective This command enables the administrative distance (that is, the metric to reach destination) of the routing protocol and sets the administrative distance value. The distance value ranges between 1 and 255.

The administrative distance can be enabled for only one route map. The distance should be disassociated for the already associated route map, if distance needs to be associated for another route map.

The no form of the command disables the administrative distance.

Syntax **distance <1-255> [route-map <name(1-20)>]**

no distance [route-map <name(1-20)>]

Parameter Description `route-map <name(1-20)>`- Configures the name of the Route Map for which the distance value should be enabled and set. This value is a string with maximum string size 20.

Mode OSPF Router Configuration Mode

Default 0 (Represents directly connected route)

Note: This command executes only if OSPF router is enabled.

Example

```
Your Product(config-router)# distance 10 route-map rmap-test
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `show ip ospf` – Displays general information about OSPF routing process

route-calculation staggering

Command Objective This command enables OSPF route calculation staggering feature and also sets the staggering interval to the last configured value. This feature staggers the OSPF route calculation at regular intervals for processing neighbor keep alive and other OSPF operations.

The no form of the command disables OSPF route calculation staggering and removes the staggering interval.

Syntax **route-calculation staggering**

no route-calculation staggering

Mode OSPF Router Configuration Mode

Default OSPF route calculation staggering is enabled.
Note: This command executes only if OSPF router is enabled.

Example

```
Your Product(config-router)# route-calculation staggering
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `route-calculation staggering-interval` - Configures the OSPF route calculation staggering interval

- `show ip ospf` – Displays general information about OSPF routing process

route-calculation staggering-interval

Command Objective This command configures the OSPF route calculation staggering interval (in milliseconds). This value represents the time after which the route calculation is suspended for doing other OSPF operations. The value ranges between 1000 to 2147483647 milliseconds.

Syntax `route-calculation staggering-interval <milli-seconds (1000-2147483647)>`

Mode OSPF Router Configuration Mode

Default 10000 milliseconds (OSPF route calculation staggering interval is equal to Hello interval)

Note: This command executes only if OSPF router is enabled.

Example `Your Product(config-router)# route-calculation staggering-interval 2000`

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `route-calculation staggering-interval` - Configures the OSPF route calculation staggering interval
- `show ip ospf` – Displays general information about OSPF routing process

network

Command Objective This command defines the interfaces on which OSPF runs and the area ID for those interfaces. When a more specific OSPF network range is removed, interfaces belonging to that network range will be retained and remain active if and only if a less specific network range exists. There is no limit to the number of network commands that can be used on the router. The IP address for the entry should be same as that of the configured interface.

The no form of the command disables OSPF routing for interfaces defined and to remove the area ID of that interface.

Syntax **network <Network number> area <area-id> [unnum { Vlan <vlan-id/vfi-id> [switch <switch-name>] | <interface-type> <interface-num> | <IP-interface-type> <IP-interface-number>}]**

no network <Network number> area <area-id> [unnum { Vlan <vlan-id/vfi-id> [switch <switch-name>] | <interface-type> <interface-num> | <IP-interface-type> <IP-interface-number>}]

Parameter Description

- `<Network number>` - Configures the Network type for the interfaces.

- `<area-id>` - Configures the area associated with the OSPF address range and the identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IP address.
- `unnum { Vlan <vlan-id/vfi-id>` - Configures the Network type for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - `<vlan -id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - `<vfi-id>`. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535

    Notes:

    1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
    2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
    3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example, if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- `switch<switch-name>` - Configures the Network type for the specified context. This value represents unique name of the switch context. This value is a string with maximum size 32.. This parameter is specific to multiple instance feature.
- `<interface-type>` - Configures the Network type for the specified type of interface. The interface can be:
  - `gigabitethernet` – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - `extreme-ethernet` – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - `qx-ethernet` – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
- `<interface-num>` - Configures the Network type for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan ID is provided, for interface types i-lan. For example: 1 represents i-lan ID.
- `<IP-interface-type>` - Configures the Network type for the specified L3 Psuedo wire interface in the system.
- `<IP-interface-number>` - Configures the Network type for the specified L3 Psuedo wire interface identifier. This is a unique value that represents the specific interface . This value ranges between 1 and 65535 for Psuedowire interface.

Note: Maximum number of PseudoWire interfaces supported in the system is 100.

Mode OSPF Router Configuration Mode

Example Your Product(config-router)# network 0.0 area 0.0 unnum Vlan 1

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `show ip ospf interface` - Displays OSPF interface information.
- `area – virtual link key start-accept` –Configuring the Start Accept Time for Cryptographic Key
- `show ip ospf - summary address` – Displays OSPF Summary-address redistribution Information
- `show ip ospf - database summary` – Displays OSPF LSA Database summary
- `area -virtual link key start-generate` – Configuring Start Generate Time for Cryptographic Key
- `area -virtual link key stop-accept` – Configuring Stop Accept Time for Cryptographic Key
- `area -virtual link key stop-generate` – Configuring Stop Generate Time for Cryptographic Key

set nssa asbr-default-route translator

Command Objective This command enables/disables setting of P bit in the default Type-7 LSA generated by NSSA internal ASBR.

Syntax **set nssa asbr-default-route translator { enable | disable }**

Parameter Description

- `enable` - Sets P-Bit in the generated Type-7 default LSA, when nssa absr is set to enabled.
- `disable` - Clears P-Bit in the generated default LAS, when nssa absr is set to disabled.

Mode OSPF Router Configuration Mode

Default Disable

Note: This command executes only if OSPF router is enabled.

Example

```
Your Product(config-router)# set nssa asbr-default-route translator enable
```

Related Command(s) `router ospf` – Enables OSPF routing process.

passive-interface vlan

Command Objective This command suppresses routing updates on an interface and makes the interface passive. OSPF routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF domain.

The no form of the command enables routing updates on an interface.

Syntax **passive-interface {vlan <vlan-id/vfi-id> [switch <switch-name>] | <interface-type> <interface-id> | <IP-interface-type> <IP-interface-number>}**

no passive-interface {vlan <vlan-id/vfi-id> [switch <switch-name>] | <interface-type> <interface-id> | <IP-interface-type> <IP-interface-number>}

Parameter Description

- `vlan <vlan-id/vfi-id>` - Configures the specified VLAN / VFI ID as passive interface.This value ranges between 1 and 65535.
  - <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535

  Notes:

  1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
  2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
  3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- switch<switch-name> - Configures ospf for the specified context. This value represents unique name of the switch context. This value is a string with maximum size 32.. This parameter is specific to multiple instance feature.
- <interface-type> - Configures ospf for the specified type of interface. The interface can be:
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
- <interface-num> - Configures ospf for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan ID is provided, for interface types i-lan. For example: 1 represents i-lan ID.
- <IP-interface-type> - Configures the specified L3 Psuedo wire interface in the system as passive interface.

- <IP-interface-number> - Configures the specified L3 Psuedo wire interface identifier as passive interface. This is a unique value that represents the specific interface . This value ranges between 1 and 65535 for Psuedowire interface.

  Note: Maximum number of PseudoWire interfaces supported in the system is 100.

Mode OSPF Router Configuration Mode

Example

```
Your Product(config-router)# passive-interface vlan 1
```

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `show ip ospf interface` - Displays OSPF interface information.
- `network` – Defines the interfaces on which OSPF runs and area ID for those interfaces.
- `passive-interface default` – Suppresses routing updates on all interfaces
- `show ip ospf request-list` – Displays OSPF Link state request list information

passive-interface default

Command Objective This command suppresses routing updates on all interfaces and makes the passive interface to default. All the OSPF interfaces after the execution of this command will be passive. This is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

The no form of the command enables routing updates on all interfaces.

Syntax **passive-interface default**

no passive-interface default

Mode OSPF Router Configuration Mode

Example

```
Your Product(config-router)# passive-interface default
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `passive-interface vlan` – Suppresses routing updates on an interface.
- `show ip ospf interface` – Displays OSPF interface information.
- `show ip ospf request-list` – Displays OSPF Link state request list information.

ip ospf demand-circuit

Command Objective This command configures OSPF to treat the interface as an OSPF demand circuit. On point-to-point interfaces, only one end of the demand circuit must be configured. This command allows the underlying data link layer to be closed when the topology is stable. It indicates whether Demand OSPF procedures (hello suppression to FULL neighbors and setting the DoNotAge flag on prorogated LSAs) must be performed on this interface.

On point-to-point interfaces, only one end of the demand circuit must be configured with this command. Periodic hello messages are suppressed and periodic refreshes of link-state advertisements (LSAs) do not flood the demand circuit. This command executes only if OSPF routing process is enabled.

The no form of the command removes the demand circuit designation from the interface.

Syntax **ip ospf demand-circuit**

no ip ospf demand-circuit

Mode Interface configuration Mode (VLAN interface / Router port)

Example

```
Your Product(config-if)# ip ospf demand-circuit
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `show ip ospf interface` – Displays OSPF interface information.

ip ospf retransmit-interval

Command Objective This command specifies the time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The value ranges between 1 and 3600. This value is also used while retransmitting database description and link-state request packets.

The no form of the command uses the default time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface.

Syntax **ip ospf retransmit-interval <seconds (1 - 3600)>**

no ip ospf retransmit-interval

Mode Interface configuration Mode (VLAN interface / Router port)

Default 5

Example

```
Your Product(config-if)# ip ospf retransmit-interval 300
```

Note: This command executes only if theOSPF routing process is enabled.

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `show ip ospf interface` – Displays OSPF interface information.

ip ospf transmit-delay

Command Objective This command sets the estimated time(in seconds) it requires to transmit a link state update packet on the interface. The value ranges between 1 and 3600. Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the seconds argument before transmission.

The no form of the command sets the default estimated time it takes to transmit a link state update packet on the interface.

Syntax **ip ospf transmit-delay <seconds (1 - 3600)>**

no ip ospf transmit-delay

Mode Interface configuration Mode (VLAN interface / Router port)

Default 1

Note: This command executes only if the OSPF routing process is enabled.

Example

```
Your Product(config-if)# ip ospf transmit-delay 50
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `show ip ospf interface` – Displays OSPF interface information.

ip ospf priority

Command Objective This command sets the router priority which helps determine the designated router for this network. When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence The number value that specifies the priority of the router ranges is from 0 to 255. When two routers attached to a network attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence.

The no form of the command sets default value for router priority.

Syntax **ip ospf priority <value (0 - 255)>**

no ip ospf priority

Mode Interface configuration Mode (VLAN interface / Router port)

Default 1

Note: This command executes only if theOSPF routing process is enabled.

Example `Your Product(config-if)# ip ospf priority 25`

Related Command(s) `router ospf` – Enables OSPF routing process.

ip ospf hello-interval

Command Objective This command specifies the interval (in seconds) between hello packets sent on the interface. This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes will be detected. The value ranges between 1 and 65535. This value must be the same for all routers attached to a common network.

The no form of the command sets default value for, interval between hello packets sent on the interface.

Syntax **ip ospf hello-interval <seconds (1 - 65535)>**

no ip ospf hello-interval

Mode Interface configuration Mode (VLAN interface / Router port)

Default 10

Note: This command executes only if theOSPF routing process is enabled.

Example

```
Your Product(config-if)# ip ospf hello-interval 75
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `show ip ospf interface` – Displays OSPF interface information.

ip ospf dead-interval

Command Objective This command sets the interval (in seconds) at which hello packets must not be seen before neighbors declare the router down. The interval is advertised in router hello packets. The value ranges between 1 and 65535.

The no form of the command sets default value for the interval at which hello packets must not be seen before neighbors declare the router down. This value must be the same for all routers and access servers on a specific network.

Syntax **ip ospf dead-interval <seconds (1-65535)>**

no ip ospf dead-interval

Mode Interface configuration Mode (VLAN interface / Router port)

Default 40

Note: This command executes only if theOSPF routing process is enabled.

Example `Your Product(config-if)# ip ospf dead-interval 1000`

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `show ip ospf interface` – Displays OSPF interface information.

ip ospf cost

Command Objective This command explicitly specifies the cost of sending a packet on an interface. The link-state metric is advertised as the link cost in the router link advertisement.

The no form of the command resets the path cost to the default value.

In general, the path cost is calculated using the following formula:

- 108 / bandwidth

Using this formula, the default path costs are calculated

- Example: 56-kbps serial link-Default cost is 1785
- Ethernet-Default cost is 10

Syntax **ip ospf cost <cost (1-65535)> [tos <tos value (0-30)>]**

no ip ospf cost [tos <tos value (0-30)>]

Parameter Description

- `<cost (1-65535)>` - Configures the Type 1 external metrics which is expressed in the same units as OSPF interface cost, that is in terms of the OSPF link state metric. This value ranges between 1 and 65535.
- `tos <tos value (0-30)>` - Configures the type of Service of the route being configured. The value ranges between 0 and 30. This parameter can be configured only if the code is compiled with TOS Support

Mode Interface configuration Mode (VLAN interface / Router port)

Default 0

Example `Your Product(config-if)# ip ospf ip ospf cost 10`

Related Command(s)

- `area-Default cost`– Specifies a cost for the default summary route sent into a stub or NSSA
- `show ip ospf interface` – Displays OSPF interface information.

ip ospf network

Command Objective This command configures the OSPF network type to a type other than the default for a given media and configures broadcast networks as NBMA networks. Each pair of routers on a broadcast network is assumed to be able to communicate directly. An Ethernet is an example of a broadcast network. A 56Kb serial line is an example of a point-to-point network.

The no form of the command sets the OSPF network type to the default type.

Syntax **ip ospf network {broadcast | non-broadcast | point-to-multipoint | point-to-point}**

no ip ospf network

Parameter Description

- `broadcast` - Configures the broadcast networks supporting many (more than two) attached routers, together with the capability to address a single physical message to all of the attached routers (broadcast)
- `non-broadcast` - Configures the non broadcast networks supporting many (more than two) routers, but having no broadcast capability Sets the network type to nonbroadcast multiaccess (NBMA).
- `point-to-multipoint` - Sets the network type to point-to-multipoint and treats the non- broadcast network as a collection of point-to-point links.
- `point-to-point` - Sets the network type to point-to-point that joins a single pair of routers.

Mode Interface configuration Mode (VLAN interface / Router port)

Default Broadcast

Example

```
Your Product(config-router)# ip ospf network broadcast
```

Related Command(s)

- `neighbor`– Specifies a neighbor router and its priority.
- `ip ospf priority` – Sets the router priority
- `show ip ospf interface` – Displays OSPF interface information.

ip ospf authentication-key

Command Objective This command specifies a password to be used by neighboring routers that are using the OSPF simple password authentication. The password created by this command is used as a key that is inserted directly into the OSPF header when the routing protocol packets are originated. The size of the password is 8 bytes. The password string can contain from 1 to 8 uppercase and lowercase alphanumeric characters. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information.

The no form of the command removes a previously assigned OSPF password.

Syntax **ip ospf authentication-key <password (8)>**

no ip ospf authentication-key

Mode Interface configuration Mode (VLAN interface / Router port)

Default 40

Note: This command executes only if theOSPF routing process is enabled.

Example

```
Your Product(config-if)# ip ospf authentication-key asdf123
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `ip ospf authentication` – Specifies the authentication type for an interface
- `show ip ospf interface` – Displays OSPF interface information.

ip ospf message-digest-key

Command Objective This command enables OSPF MD5 authentication. One key per interface is used to generate authentication information when sending packets and to authenticate incoming packets.

The no form of the command removes an old MD5 key.

- 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.
- Usually, one key per interface 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.

Syntax **ip ospf message-digest-key <Key-ID (0-255)> [{ md5 | sha-1 | sha-224 | sha-256 | sha-384 | sha-512}] <Key (16)>**

no ip ospf message-digest-key <Key-ID (0-255)>

Parameter Description

- <Key-ID(0-255)> - Configures the secret key, which is used to create the message digest appended to the OSPF packet. The value ranges between 0 and 255.

- md5 - Sets the authentication type as Message Digest 5 (MD5) authentication.

- sha-1 - Sets the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes.

- sha-224 - Sets the authentication type as Secure Hash Algorithm 224 (SHA224) authentication. SHA224 generates Authentication digest of length 28 bytes.

- sha-256 - Sets the authentication type as Secure Hash Algorithm 256 (SHA256) authentication. SHA256 generates Authentication digest of length 32 bytes.

- sha-384 - Sets the authentication type as Secure Hash Algorithm 384 (SHA384) authentication. SHA384 generates Authentication digest of length 48 bytes.

- sha-512 - Sets the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. SHA512 generates Authentication digest of length 64 bytes.

- <key (16)> - Configures the cryptographic key value which is used used to create the message digest appended to the OSPF packet. All neighboring routers on the same network must have the same key identifier and key to route OSPF traffic. This is a sting with maximum string size 16.

Mode Interface configuration Mode (VLAN interface / Router port)

Notes:

- This command executes only if theOSPF routing process is enabled.
- The authentication type should be the same as set in the ip ospf authentication command

Example

```
Your Product(config-router)# ip ospf message-digest-key 20 sha-256 abcd
```

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `ip ospf authentication` - Specifies the authentication type for an interface.
- `show ip ospf interface` – Displays OSPF interface information.

ip ospf authentication

Command Objective This command specifies the authentication type for an interface and the no form of the command removes the authentication type for an interface and set it to NULL authentication.

Syntax **ip ospf authentication [{message-digest | sha-1 | sha-224 | sha-256 | sha-384 | sha-512 | null | simple}]**

no ip ospf authentication

Parameter Description

- `message-digest` - Sets the authentication type as message-digest authentication.
- `sha-1` - Sets the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes.
- `sha-224` - Sets the authentication type as Secure Hash Algorithm 224 (SHA224) authentication.

SHA224 generates Authentication digest of length 28 bytes.

- sha-256 - Sets the authentication type as Secure Hash Algorithm 256 (SHA256) authentication. SHA256 generates Authentication digest of length 32 bytes.
- sha-384 - Sets the authentication type as Secure Hash Algorithm 384 (SHA384) authentication. SHA384 generates Authentication digest of length 48 bytes.
- sha-512 - Sets the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. SHA512 generates Authentication digest of length 64 bytes.
- null - Sets the authentication type as null authentication which is used for overriding password or message-digest authentication if configured for an area.
- simple – Sets the authentication type as simple password authentication mechanism.

Mode Interface configuration Mode (VLAN interface / Router port)

Default NULL

Note: This command executes only if theOSPF routing process is enabled.

Example

```
Your Product(config-if)# ip ospf authentication
```

Related Command(s)

- router ospf – Enables OSPF routing process
- ip ospf message-digest-key - Enables OSPF MD5 authentication
- area - virtual-link – Defines an OSPF virtual link and its related parameters
- ip ospf authentication-key – Specifies a password to be used by neighboring routers that are using the OSPF simple password authentication
- show ip ospf interface – Displays OSPF interface information.

debug ip ospf

Command Objective This command sets the OSPF debug level.

The no form of this command disables the debug function

Syntax **debug ip ospf [vrf <name>] { pkt { hp | ddp | lrq | lsu | lsa } | module { adj_formation | ism | nsm | config | interface | restarting-router | helper | redundancy } }**

no debug ip ospf [vrf <name>] { pkt { hp | ddp | lrq | lsu | lsa } | module { adj_formation | ism | nsm | config | interface | restarting-router | helper | redundancy } | all }

Parameter Description

- vrf<name> - Sets ospf debug level for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size 32.
- pkt - Generates debug statements for Packet High Level Dump trace
  - hp - Generates debug statements for Hello packet traces

    - ddp - Generates debug statements for DDP packet traces
    - lrq - Generates debug statements for Link State Request Packet traces
    - lsu - Generates debug statements for Link State Update Packet traces
    - lsa - Generates debug statements for Link State Acknowledge Packet traces
- module - Generates debug statements for RTM Module traces
    - adj_formation - Generates debug statements for Adjacency formation traces
    - ism - Generates debug statements for Interface State Machine traces
    - nsm - Generates debug statements for Neighbor State Machine traces
    - config - Generates debug statements for Configuration traces
    - interface - Generates debug statements for Interface
    - restarting-router - Generates debug statements for messages related to restarting router
    - helper - Generates debug statements for messages related to router in helper Mode
    - redundancy - Generates debug statements for redundancy messages.
- all - Generates debug statements for all messages.

Mode Privileged EXEC Mode

Example `Your Product# debug ip ospf pkt hp`

Related Command(s)

- ip vrf - Creates VRF instance.
- show debugging – Displays the state of each debugging option.

show ip ospf

Command Objective This command displays general information about the OSPF routing process.

Syntax **show ip ospf [vrf <name>]**

Parameter Description vrf <name> - Displays the general information of ospf for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip ospf
OSPF Router with ID (0.0.0.0) (Vrf default) Supports only single TOS(TOS0) route Opaque
LSA Support : Disabled
ABR Type supported is Standard ABR Autonomous System Boundary Router : Disabled
P-B it setting for the default Type-7 LSA that needs to be generated by the ASBR(which is
not ABR) is disabled
Non-Stop Forwarding disabled Restart-interval limit: 120
Grace LSA Retransmission Count: 2 Helper Grace LSA ACK :Required Restart Reason is:
Unknown
Helper is Giving Support for: Unknown
```

```
Software Restart
Software Reload/Upgrade
Switch To Redundant
Helper Grace Time Limit: 0
Strict LSA checking State Is:Disabled Route calculation staggering is enabled
Route calculation staggering interval is -1718520588 milliseconds
Redistributing External Routes is disabled
Default passive-interface Disabled
Rfc1583 compatibility is enabled
Administrative Distance is 110
Number of Areas in this router is 0
Default information originate is disabled
                                              BFD is disabled
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `router-id` – Sets the router-id for the OSPF process
- `area – nssa` - Configures an area as a not-so-stubby area (NSSA)
- `area - Stability interval` – Configures the Stability interval for NSSA
- `area - virtual-link` – Defines an OSPF virtual link and its related parameters
- `nsf ietf restart-support` - Enables the graceful restart support
- `nsf ietf restart-interval` - Configures the OSPF graceful restart timeout interval
- `nsf ietf helper-support` - Enables the helper support
- `nsf ietf helper gracetimelimit` - Configures the graceful restart interval limit in helper side
- `nsf ietf helper strict-lsa-checking` - Enables the strict LSA check option in helper
- `nsf ietf grace lsa ack required` - Enables Grace Ack Required state in restarter
- `nsf ietf grlsa retrains count` – Configures the maximum of retransmissions for unacknowledged GraceLSA.
- `nsf ietf restart-reason` - Configures the reason for graceful restart
- `route-calculation staggering` - Enables OSPF route calculation staggering feature
- `route-calculation staggering-interval` - Configures the OSPF route calculation staggering interval
- `ip ospf authentication-key` – Specifies a password to be used by neighboring routers that are using the OSPF simple password authentication
- `ip ospf start-accept key` - Configures the time the router will start accepting packets that have been created with the specified key
- `ip ospf stop-accept key` - Configures the time the router will stop accepting packets that have been created with the specified key
- `ip ospf start-generate key` - Configures the time the router will start generating packets that have been created with the specified key
- `ip ospf stop-generate key` - Configures the time the router will stop generating packets that have been created with the specified key
- `enable bfd` - Enables BFD feature in OSPF
- `disable bfd` - Disables BFD feature in OSPF

show ip ospf - interface

Command Objective This command displays the general information of OSPF routing processes for the specified interface.

Syntax **show ip ospf [vrf <name>] interface [{ vlan <vlan-id/vfi-id> [switch <switch-name>] | <interface-type> <interface-id> | <IP-interface-type> <IP-interface-number>}]**

Parameter Description

- `vrf<name>` - Displays the interface general information of OSPF for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size 32.
- `vlan <vlan-id/vfi-id>` - Displays the interface general information of OSPF for the specified VLAN / VFI ID.This value ranges between 1 and 65535.
  - `<vlan -id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - `<vfi-id>`. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535

    Notes:

    1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
    2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
    3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- switch<switch-name> - Displays ospf for the specified context. This value represents unique name of the switch context. This value is a string with maximum size 32. This parameter is specific to multiple instance feature.
- <interface-type> - Configures ospf for the specified type of interface. The interface can be:
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
- <interface-id> - Displays ospf for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan ID is provided, for interface

types i-lan. For example: 1 represents i-lan ID.

- <IP-interface-type> - Displays ospf configuration in the specified L3 Psuedo wire interface in the system.
- <IP-interface-number> - Displays ospf configuration for the specified interface identifier. This is a unique value that represents the specific interface . This value ranges between 1 and 65535 for Psuedowire interface.

Note: Maximum number of PseudoWire interfaces supported in the system is 100.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip ospf interface vlan 1
Vlan1 is line protocol is up
Internet Address 13.0.0.1, Mask 255.0.0.0, Area 0.0.0.0
AS 1, Router ID 12.0.0.2, Network Type BROADCAST, Cost 1
demand circuit is disabled
Transmit Delay is 1 sec, State 4, Priority 1
Designated RouterId 12.0.0.2, Interface address 13.0.0.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
Hello due in 1 sec
Neighbor Count is 0, Adjacent neighbor count is 0
sha-1                   authentication enabled
sha-1 authentication key is configured
Youngest key id is 1
Key Start Accept Time   is 26-Jun-2013,02:50
Key Start Generate Time is 26-Jun-2013,02:50
Key Stop Generate Time  is 06-Feb-2136,06:28
Key Stop Accept Time    is 06-Feb-2136,06:28
Simple Authentication   Key is not Configured
Connected to VRF        default
Bfd Enable
```

Related Command(s)

- `area - nssa` - Configures an area as a not-so-stubby area (NSSA)
- `network`– Defines the interfaces on which OSPF runs and to define the area ID for those interfaces
- `passive-interface vlan` – Suppresses routing updates on an interface
- `passive-interface default` – Suppresses routing updates on all interface
- `ip ospf demand-circuit` – Configures OSPF to treat the interface as as an OSPF demand circuit
- `ip ospf hello-interval` – Specifies the interval between hello packets sent on the interface
- `ip ospf dead-interval` – Sets the interval at which hello packets must not be seen before neighbors declare the router down
- `ip ospf cost` – Specifies the cost of sending a packet on an interface
- `bfd` – Enables BFD monitoring on all or specifc OSPF interfaces
- `ip ospf bfd` – Sets BFD support on the interface

show ip ospf - neighbor

Command Objective This command displays OSPF-related neighbor information list and observes the neighbor data structure.

Syntax **show ip ospf [vrf <name>] neighbor [{ vlan <vlan-id/vfi-id> [switch <switch-name>] | <interface-type> <interface-id> | <IP-interface-type> <IP-interface-number>}] [Neighbor ID] [detail]**

Parameter Description

- vrf<name> - Displays OSPF-related neighbor information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size 32.
- vlan <vlan-id/vfi-id> - Displays OSPF-related neighbor information for the specified VLAN / VFI ID.This value ranges between 1 and 65535.
  - <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
  - <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535

    Notes:

    1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
    2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
    3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- switch<switch-name> - Displays OSPF-related neighbor information for the specified context. This value represents unique name of the switch context. This value is a string with maximum size 32. This parameter is specific to multiple instance feature.
- <interface-type> - Displays OSPF-related neighbor information for the specified type of interface. The interface can be:
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
- <interface-id> - Displays OSPF-related neighbor information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot

number and port number separated by a slash, for interface type other than i-lan and port- channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan ID is provided, for interface types i-lan. For example: 1 represents i-lan ID.

- <IP-interface-type> - Displays OSPF-related neighbor information for the specified L3 Psuedo wire interface in the system.
- <IP-interface-number> - Displays OSPF-related neighbor information for the specified interface identifier. This is a unique value that represents the specific interface . This value ranges between 1 and 65535 for Psuedowire interface.

  Note: Maximum number of PseudoWire interfaces supported in the system is 100.

- Neighbor ID - Displays the neighbor router ID
- detail - Displays the OSPF Neighbor information in detail

Mode Privileged EXEC Mode

Example

```
Your Product# show ip ospf neighbor
Vrf default
Neighbor-ID Pri  State      DeadTime  Address
Interface Helper   HelperAge   HelperER   Bfd
-----------------  -----  --------         -------------  -----------     -----
---------- ---------------  -------------------  --------------  --------
12.0.0.1      1    FULL/BACKUP   30         20.0.0.1
vlan2   Not Helping  0              None      Enabled
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `neighbor` – Specifies a neighbor router and its priority.
- `enable bfd` - Enables BFD feature in OSPF
- `disable bfd` – Disables BFD feature in OSPF
- `router-id` – Sets the router-id for the OSPF process
- `network` – Defines the interfaces on which OSPF runs and area ID for those interfaces

show ip ospf - request-list

Command Objective This command displays OSPF Link state request list advertisements (LSAs) requested by a router and debugging OSPF routing operations.

Syntax **show ip ospf [vrf <name>] request-list [<neighbor-id>] [{ vlan <vlan-id/vfi-id> [switch <switch-name>] | <interface-type> <interface-id> | <IP-interface-type> <IP-interface-number>}]**

Parameter Description

- vrf<name> - Displays ospf for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size 32.

- <neighbor-id> - Displays OSPF request LSAs for the sepcified neighbor router ID.
- vlan <vlan-id/vfi-id> - Displays OSPF request LSAs for the specified VLAN / VFI ID.This value ranges between 1 and 65535.
    - <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
    - <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535

      Notes:

      1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
      2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
      3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.
- switch<switch-name> - Displays OSPF for the specified context. This value represents unique name of the switch context. This value is a string with maximum size 32. This parameter is specific to multiple instance feature.
- <interface-type> - Displays OSPF for the specified type of interface. The interface can be:
    - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
    - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
    - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
- <interface-id> - Displays OSPF for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan ID is provided, for interface types i-lan. For example: 1 represents i-lan ID.
- <IP-interface-type> - Displays OSPF configuration in the specified L3 Psuedo wire interface in the system.
- <IP-interface-number> - Displays OSPF-related neighbor information for the specified interface identifier. This is a unique value that represents the specific interface . This value ranges between 1 and 65535 for Psuedowire interface.

  Note: Maximum number of PseudoWire interfaces supported in the system is 100.

Mode Privileged EXEC Mode

Example

```
Single Instance:
Your Product# show ip ospf request-list vlan 1
OSPF Router with ID (20.0.0.2)
Neighbor 10.0.0.1, interface vlan1 address 40.0.0.1
Type LS-ID     ADV-RTR              Age     Checksum
------- -------      -----------      --------      -----     ------------
Neighbor 20.0.0.2, interface vlan1 address 40.0.0.2
Type LS-ID     ADV-RTR     SeqNo     Age     Checksum
---- ----      -------     -----     ---     --------
Multiple Instance:
Your Product# show ip ospf request-list
OSPF Router with ID (10.0.0.1) (Vrf default )
Neighbor 10.0.0.2, interface - address 10.0.0.2
Type LS-ID     ADV-RTR     SeqNo     Age     Checksum
Neighbor 11.0.0.1, interface - address 11.0.0.1
Type LS-ID     ADV-RTR     SeqNo     Age     Checksum
Neighbor 13.0.0.3, interface - address 13.0.0.3
Type LS-ID     ADV-RTR     SeqNo     Age     Checksum
Neighbor 14.0.0.4, interface - address 14.0.0.4
Type LS-ID     ADV-RTR     SeqNo     Age     Checksum
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `router-id` – Sets the router-id for the OSPF process
- `passive-interface vlan` – Suppresses routing updates on an interface
- `passive-interface default` – Suppresses routing updates on all interfaces

show ip ospf - retransmission-list

Command Objective This command displays list of all OSPF Link state retransmission list information waiting to be resent. This value is also used while retransmitting database description and link-state request packets.

Syntax **show ip ospf [vrf <name>] retransmission-list [<neighbor-id>] [{ vlan <vlan-id/vfi-id> [switch <switch-name>] | <interface-type> <interface-id> | <IP-interface-type> <IP-interface-number>}]**

Parameter Description

- vrf<name> - Displays ospf for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size 32.
- <neighbor-id> - Configures the neighbor router ID
- vlan <vlan-id/vfi-id> - Displays retransmission list information for the specified VLAN / VFI ID.This value ranges between 1 and 65535.
    - -<vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094

- <vfi-id>. - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports . This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535

  Notes:

  1. The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering Database entries.
  2. VFI IDs 4096 and 4097 are reserved identifiers used in MPLS PW.
  3. The theoretical maximum for the maximum number of VFI is 65535 but the actual number of VFI supported is a sizing constant. Based on this, the maximum number of VFI ID accepted in the management interface is restricted. For example if 100 VFIs are supported, the maximum number of VFI supported will be restricted to maximum number of VLANs + 100. An error message is displayed for any value beyond this range.

- switch<switch-name> - Displays ospf for the specified context. This value represents unique name of the switch context. This value is a string with maximum size 32. This parameter is specific to multiple instance feature.
- <interface-type> - Displays ospf for the specified type of interface. The interface can be:
  - gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second.
  - extreme-ethernet – A version of Ethernet that supports data transfer upto 10 Gigabits per second. This Ethernet supports only full duplex links.
  - qx-ethernet – A version of Ethernet that supports data transfer upto 40 Gigabits per second. This Ethernet supports only full duplex links.
- <interface-id> - Displays ospf for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan ID is provided, for interface types i-lan. For example: 1 represents i-lan ID.
- <IP-interface-type> - Displays ospf configuration in the specified L3 Psuedo wire interface in the system.
- <IP-interface-number> - Displays ospf configuration for the specified interface identifier. This is a unique value that represents the specific interface . This value ranges between 1 and 65535 for Psuedowire interface.

  Note: Maximum number of PseudoWire interfaces supported in the system is 100.

Mode Privileged EXEC Mode

Example

```
Single Instance:
Your Product# show ip ospf retransmission-list vlan 1
OSPF Router with ID (20.0.0.2)
Neighbor 10.0.0.1, interface vlan1 address 10.0.0.2
Queue length 3
```

```
Type LS-ID     ADV-RTR  SeqNo      Age Checksum
1    20.0.0.2  20.0.0.2  0x80000006 0  0x522f
Multiple Instance:
Your Product# show ip ospf retransmission-list vlan 1
OSPF Router with ID (11.0.0.1) (Vrf default )
Neighbor 10.0.0.1, interface vlan1 address 10.0.0.2
Link State retransmission due in  30 ticks, Queue length 3
Type LS-ID     ADV-RTR  SeqNo  Age Checksum
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `router-id` – Sets the router-id for the OSPF process
- `ip ospf retransmit-interval` – Specifies the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface.

show ip ospf - virtual-links

Command Objective This command display parameters, and the current state of OSPF virtual links.

Syntax **show ip ospf [vrf <name>] virtual-links**

Parameter Description `vrf<name>`- Displays ospf for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size 32.

Mode Privileged EXEC Mode

Example

```
Single Instance:
Your Product# show ip ospf virtual-links
Virtual Link to router 10.0.0.1, Interface State is DOWN
Transit Area 33.0.0.12
Transmit Delay is 1 sec, Neighbor State DOWN
Timer intervals configured, Hello 10, Dead 60,
Retransmit 5
Multiple Instance:
Your Product# show ip ospf virtual-links
Vrf   default
Virtual Link to router 11.0.0.1, Interface State is DOWN
   Transit Area 1.1.1.1
   Transmit Delay is 1 sec, Neighbor State DOWN
 Timer intervals configured, Hello 10, Dead 60,
Retransmit 5
Virtual Link to router 16.0.0.6, Interface State is DOWN
   Transit Area 5.5.5.5
   Transmit Delay is 1 sec, Neighbor State DOWN
 Timer intervals configured, Hello 10, Dead 60,

Retransmit 5
```

Related Command(s) `area - virtual-link` – Defines an OSPF virtual link and its related parameters

show ip ospf - border-routers

Command Objective This command displays the internal OSPF routing table entries to an Area Border Router and Autonomous System Boundary Router.

Syntax **show ip ospf [vrf <name>] border-routers**

Parameter Description `vrf<name>`- Displays ospf for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip ospf border-routers
Vrf   default
OSPF Process Border Router Information
Destination  TOS  Type   NextHop     Cost   Rt.Type
Area
-----------  ---  -----  ----------  -----  ----------
-------
12.0.0.2     0    ASBR   12.0.0.2    1       intraArea
0.0.0.0
```

Related Command(s)

- `abr-type` – Sets the Alternative ABR Type
- `ASBR Router` – Specifies this router as ASBR

show ip ospf - summary address

Command Objective This command displays OSPF summary-address redistribution information configured under an OSPF process.

Syntax **show ip ospf [vrf <name>] {area-range | summary-address}**

Parameter Description

- `vrf<name>` - Displays ospf for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size 32.
- `area-range` - Displays the area associated with the OSPF address range.
- `summary-address` - Displays the aggregate addresses for OSPF

Mode Privileged EXEC Mode

Example

```
Single Instance:
Your Product# show ip ospf area-range
Display of Summary addresses for Type3 and Translated
```

```
Type5
Summary Address
----------------------------------------------
Network  Mask      LSAType Area     Effect   Tag
-------  -------     -------          ------   -----
255.0.0.0 Summary 33.0.0.12 Advertise 1074636208
Your Product# show ip ospf summary-address
Display of Summary addresses for Type3 and Type7 from
Redistributed routes
OSPF External Summary Address Configuration Information
--------------------------------------------------------
Network  Mask     Area           Effect    TranslationSt
-------  ----     ----           ------    -------------
10.0.0.1 255.0.0.0 33.0.0.12    advertiseMatching enabled
Multiple Instance:
Your Product# show ip ospf summary-address
Display of Summary addresses for Type3 and Type7 from
Redistributed routes
Vrf  default
OSPF External Summary Address Configuration Information
------------------------------------------------------
Network  Mask     Area     Effect   TranslationSt
--------------------------------------------------
11.0.0.9 255.0.0.0  0.0.0.0     AllowAll    enabled
16.0.0.1 255.0.0.0  0.0.0.0     AllowAll    enabled
```

Related Command(s)

- `area - range` – Consolidates and summarizes routes at an area boundary
- `summary-address` – Creates aggregate addresses for OSPF

show ip ospf - route

Command Objective This command displays routes learnt by OSPF process.

Syntax show ip ospf [vrf <name>] route

Parameter Description `vrf<name>`- Displays ospf for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip ospf route
OSPF Routing Table  Vrf  default
Dest/Mask          TOS NextHop/Interface Cost Rt.Type
Area
---------          ----- -------/--------- ------- -------
-------
12.0.0.0/255.0.0.0 0   0.0.0.0/vlan1   1   IntraArea
0.0.0.0
20.0.0.0/255.0.0.0  0  12.0.0.2/vlan1  10   Type2Ext
```

```
0.0.0.0
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `router-id` – Sets the router-id for the OSPF process.

show ip ospf - database

Command Objective This command displays OSPF LSA Database summary.

Syntax **show ip ospf [vrf <name>] [area-id] database [{database-summary | self-originate | adv-router <ip-address>}]**

Parameter Description

- `vrf<name>` - Displays ospf for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size 32.
- `area-id`- Displays the area associated with the OSPF address range. It is specified as an IP address.
- `database-summary` - Displays total number of each type of LSA for each area there are in the database, and the total number of LSA types.
- `self-originate` - Displays only self-originated LSAs (from the local router).
- `adv-router<ip-address>` - Displays all the specified router link-state advertisements (LSAs).

Mode Privileged EXEC Mode

Example

```
Your Product# show ip ospf database database-summary
OSPF Router with ID (12.0.0.1) (Vrf  default)
Router Link States (Area 0.0.0.0)
---------------------------------------
Link ID    ADV Router   Age  Seq#    Checksum  Link
count
----------             ---          -------
---
12.0.0.1   12.0.0.1      48   0x80000002  0xd129   1
12.0.0.2   12.0.0.2      50   0x80000002  0xcf28   1
              Network Link States (Area 0.0.0.0)
Link ID     ADV Router    Age    Seq#          Checksum
-------     ----------    ---    ----          --------
12.0.0.2   12.0.0.2       49   0x80000001      0x629f
OSPF Router with ID (14.0.0.1) (Vrf  vr1)
Your Product# show ip ospf vrf default database
OSPF Router with ID (12.0.0.1) (Vrf  default)
Router Link States (Area 0.0.0.0)
---------------------------------------
Link ID    ADV Router   Age  Seq#    Checksum  Link
count
----------                          -------
---
12.0.0.1   12.0.0.1     62    0x80000002  0xd129   1
```

```
12.0.0.2   12.0.0.2      64    0x80000002  0xcf28   1
                Network Link States (Area 0.0.0.0)
--------------------------------------------------------------
Link ID      ADV Router     Age     Seq#
Checksum
-----------      ---------------    -----    -------           ----------
---
12.0.0.2   12.0.0.2       63    0x80000001       0x629f
```

Related Command(s)

- `router ospf` – Enables OSPF routing process.
- `router-id` – Sets the router-id for the OSPF process.
- `summary-address` – Creates aggregate addresses for OSPF

show ip ospf – database summary

Command Objective This command displays OSPF Database summary for the LSA type.

Syntax **show ip ospf [vrf <name>] [area-id] database { asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router | summary } [link-state-id] [{adv-router <ip-address> | self-originate}]**

Parameter Description

- `vrf<name>` - Displays ospf for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size 32.
- `area-id`- Displays the area associated with the OSPF address range. It is specified as an IP address.
- `asbr-summary` - Displays information only about the Autonomous System Boundary Router (ASBR) summary LSAs.
- `external` - Displays information only about the external LSAs.
- `network` - Displays information only about the network LSAs
- `nssa-external` - Displays information about the NSSA external LSAs
- `opaque-area` - Displays information about the Type-10 LSAs
- `opaque-as` - Displays information about the Type-11 LSAs.
- `opaque-link` - Displays information about the Type-9 LSAs
- `router` - Displays information only about the router LSAs
- `summary` - Displays information only about the summary LSAs
- `link-state-id` - Displays the portion of the Internet environment that is being described by the advertisement. The value entered depends on the type of the LSA. The value must be entered in the form of an IP address
- `adv-router <ip-address>` - Displays all the specified router link-state advertisements (LSAs).
- `self-originate` - Displays only self-originated LSAs (from the local router)

Mode Privileged EXEC Mode

Example

```
Single Instance:
Your Product# show ip ospf database external
OSPF Router with ID (10.0.0.1)
Summary Link States (Area 33.0.0.12)
-----------------------------------------------------------
LS age              : 300
Options             : (No ToS Capability, DC)
LS Type             : Summary Links(Network)
Link State ID       : 10.0.0.0
Advertising Router  : 10.0.0.1
LS Seq Number       : 0x80000002
Checksum            : 0xae77
Length              : 28
Your Product# show ip ospf database network
OSPF Router with ID (20.0.0.2)
Summary Link States (Area 33.0.0.12)
-----------------------------------------------------------
LS age              : 900
Options             : (No ToS Capability, DC)
LS Type             : Network Links
Link State ID       : 40.0.0.2
Advertising Router  : 20.0.0.2
LS Seq Number       : 0x80000001
Checksum            : 0xce09
Length              : 32
Multiple Instance:
Your Product# show ip ospf database external
OSPF Router with ID (10.0.0.1) (Vrf  default)
Router Link States (Area 0.0.0.0)
----------------------------------------------------------------
Link ID    ADV Router   Age  Seq#    Checksum  Link
count
-------------------
---
10.0.0.1   10.0.0.1     900   0x80000009  0xde6   1
14.0.0.4   14.0.0.4     900   0x80000008  0x8f33    2
              Network Link States (Area 0.0.0.0)
----------------------------------------------------------------
Link ID     ADV Router    Age    Seq#
Checksum
------------   ----------------   -----   -------         ----------
-
14.0.0.1   10.0.0.1      1200   0x80000003      0x8e71
              Summary Link States (Area 0.0.0.0)
----------------------------------------------------------------
Link ID     ADV Router    Age    Seq#          Checksum
--------------------------------------   ----------------------------------------------------------
13.0.0.0    10.0.0.1       300   0x80000003      0x859c
11.0.0.9    10.0.0.1       900   0x80000016      0x1fe8
20.10.10.10 10.0.0.1       900   0x80000001      0x3db8
10.0.0.0    10.0.0.1       300   0x80000002      0xae77
16.0.0.1    10.0.0.1       900   0x80000016      0x2edc
17.0.0.0    10.0.0.1       900   0x80000001      0x55ca
21.0.0.0    10.0.0.1       900   0x80000001      0x21fa
```

```
15.0.0.4     14.0.0.4       900    0x8000000d       0xf812
             ASBR Summary Link States (Area 0.0.0.0)
--------------------------------------------------------------
Link ID      ADV Router     Age    Seq#             Checksum
-----------  -------------- -----  -------          ----------
11.0.0.1     10.0.0.1       1200   0x80000001       0x8b98
             Router Link States (Area 1.1.1.1)
---------------------------------------------------------
Link ID      ADV Router     Age    Seq#     Checksum  Link count
---------------------------  ---------------------------------------------------
10.0.0.1     0.0.0.1        1200   0x80000007  0x4ba8    1
11.0.0.1     11.0.0.1       1200   0x80000007  0xc139    1
```

```
             Network Link States (Area 1.1.1.1)
--------------------------------------------------------------
Link ID      ADV Router     Age    Seq#             Checksum
-----------  -------------- -----  -------          ----------
11.0.0.1     11.0.0.1       1200   0x80000003       0x5daa
               Summary Link States (Area 1.1.1.1)
-------------------------------------------------------
Link ID      ADV Router     Age    Seq#             Checksum
---------------------------  ----------            ----------
13.0.0.0     10.0.0.1        300   0x80000003       0x859c
20.10.10.10  10.0.0.1        900   0x80000002       0x3bb9
10.0.0.0     10.0.0.1        300   0x80000002       0xae77
16.0.0.1     10.0.0.1        900   0x80000016       0x2edc
17.0.0.0     10.0.0.1        900   0x80000001       0x55ca
14.0.0.0     10.0.0.1        300   0x80000003       0x78a8
21.0.0.0     10.0.0.1        900   0x80000001       0x21fa
18.0.0.0     10.0.0.1        900   0x80000001       0x52cb
15.0.0.0     10.0.0.1       1200   0x80000001       0x79a7
            NSSA External Link States (Area 4.4.4.4)
----------------------------------------------------------------
Link ID      ADV Router     Age    Seq#             Checksum
---------------------------  ----------            ----------
19.0.0.0     10.0.0.1        300   0x80000002       0x89f4
16.0.0.0     10.0.0.1        300   0x80000002       0xb0d0
13.0.0.0     10.0.0.1        300   0x80000002       0xd7ac
10.0.0.1     10.0.0.1        300   0x80000002       0xfe88
```

Related Command(s)

- `summary-address` – Defines the interfaces on which OSPF runs and to define the area ID for those interfaces.
- `router ospf` – Enables OSPF routing process.

show ip ospf redundancy

Command Objective This command displays OSPFv2 redundancy information.

Syntax show ip ospf redundancy

Mode Privileged EXEC Mode

Example

```
Your Product# show ip ospf redundancy
Redundancy Summary
-----------------------------
Hotstandby admin status : Enabled Hotstandby
state : Active and Standby Up Hotstandby bulk
update status : Completed Number of hello PDUs
synced : 0
Number of LSAs synced : 0
```

Related Command(s) `router ospf` – Enables OSPF routing process.

ip ospf key start-accept

Command Objective This command configures the time the router will start accepting packets that have been created with the specified key.

Syntax ip ospf key <Key-ID (0-255)> start-accept <DD-MON-YEAR,HH:MM>

Parameter Description

- `key <Key-ID (0-255)>` - Identifies the secret key used to create the message digest appended to the OSPF packet. This value ranges between 0 and 255.
- `start-accept <DD-MON-YEAR,HH:MM>` - Configures time the router will start accepting packets that have been created with this key. The value shown will be the sum of configured time and the system time at which the start-accept value is configured.Time is configured in 24 hours format.

  Note: System reuses the old mib objects which operate in integer format and thereby, CLI user defined format is converted by the system to be compatible to mib format. This may reflect mismatch in default values of the mib & system.

Mode Interface configuration Mode (VLAN interface / Router port)

Note: This command executes only if,

- OSPF routing process is enabled.
- Authentication key for Simple Password Authentication is removed.
- OSPF Message Digest authentitication is enabled and authentication type is specified for the interface.

Example `Your Product(config-if)# ip ospf key 5 start-accept 13-jan-2012,19:18`

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `network` - Defines the interfaces on which OSPF runs and the area ID
- `no ip ospf authentication key` – Removes a previously assigned OSPF password.

- `ip ospf message-digest-key` - Enables OSPF MD5 authentication
- `ip ospf authentication message-digest` - Specifies the authentication type for an interface
- `show ip ospf` – Displays general information about OSPF routing process
- `show ip ospf interface` - Displays OSPF interface information

ip ospf key start-generate

Command Objective This command configures the time when the switch will start generating ospf packets with same key id on the interface.

Syntax **ip ospf key <Key-ID (0-255)> start-generate <DD-MON-YEAR,HH:MM>**

Parameter Description

- `key <Key-ID (0-255)>` - Identifies the secret key used to create the message digest appended to the OSPF packet. This value ranges between 0 and 255.
- `start-accept <DD-MON-YEAR,HH:MM>` - Configures the time when the switch will start generating ospf packets with same key id. The value shown will be the sum of configured time and the system time at which the start-generate value is configured. Time will be configured in 24 hours format. Default value is current system time.

  Note: System reuses the old mib objects which operate in integer format and thereby, CLI user defined format is converted by the system to be compatible to mib format. This may reflect mismatch in default values of the mib & system.

Mode Interface configuration Mode (VLAN interface / Router port)

Note: This command executes only if ,

- OSPF routing process is enabled.
- Authentication key for Simple Password Authentication is removed.
- OSPF Message Digest authentitication is enabled and authentication type is specified for the interface.

Example

```
Your Product(config-if)# ip ospf key 5 start-generate 13-jan-2012,19:18
```

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `network` - Defines the interfaces on which OSPF runs and the area ID
- `no ip ospf authentication key` – Removes a previously assigned OSPF password.
- `ip ospf message-digest-key` - Enables OSPF MD5 authentication
- `ip ospf authentication message-digest` - Specifies the authentication type for an interface
- `show ip ospf` – Displays general information about OSPF routing process
- `show ip ospf interface` - Displays OSPF interface information

ip ospf key stop-generate

Command Objective This command configures the time when the router will stop using configured key for packet generation.

Syntax **ip ospf key <Key-ID (0-255)> stop-generate <DD-MON-YEAR,HH:MM>**

Parameter Description

- `key <Key-ID (0-255)>` - Identifies the secret key used to create the message digest appended to the OSPF packet. This value ranges between 0 and 255.
- `start-accept <DD-MON-YEAR,HH:MM>` - Configures the time when the switch will stop generating ospf packets with same key id. Time will be configured in 24 hours format. Default value is current system time.

  Note: System reuses the old mib objects which operate in integer format and thereby, CLI user defined format is converted by the system to be compatible to mib format. This may reflect mismatch in default values of the mib & system.

Mode Interface configuration Mode (VLAN interface / Router port)

Note: This command executes only if ,

- OSPF routing process is enabled.
- Authentication key for Simple Password Authentication is removed.
- OSPF Message Digest authentitication is enabled and authentication type is specified for the interface.

Example

```
Your Product(config-if)# ip ospf key 5 start-generate 13-jan-2012,19:18
```

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `network` - Defines the interfaces on which OSPF runs and the area ID
- `no ip ospf authentication key` – Removes a previously assigned OSPF password.
- `ip ospf message-digest-key` - Enables OSPF MD5 authentication
- `ip ospf authentication message-digest` - Specifies the authentication type for an interface
- `show ip ospf` – Displays general information about OSPF routing process
- `show ip ospf interface` - Displays OSPF interface information

ip ospf key stop-accept

Command Objective This command configures the time when the router will stop accepting OSPF packets created by using the configured key.

Syntax **ip ospf key <Key-ID (0-255)> stop-accept <DD-MON-YEAR,HH:MM>**

Parameter Description

- key <Key-ID (0-255)> - Identifies the secret key used to create the message digest appended to the OSPF packet. This value ranges between 0 and 255.
- start-accept <DD-MON-YEAR,HH:MM> - Configures the time when the switch will stop accepting ospf packets with same key id. Time will be configured in 24 hours format.

  Note: System reuses the old mib objects which operate in integer format and thereby, CLI user defined format is converted by the system to be compatible to mib format. This may reflect mismatch in default values of the mib & system.

Mode Interface configuration Mode (VLAN interface / Router port)

Note: This command executes only if ,

- OSPF routing process is enabled.
- Authentication key for Simple Password Authentication is removed.
- OSPF Message Digest authentitication is enabled and authentication type is specified for the interface.

Example

```
Your Product(config-if)# ip ospf key 5 stop-accept 13-jan-2012,19:18
```

Related Command(s)

- router ospf – Enables OSPF routing process
- network - Defines the interfaces on which OSPF runs and the area ID
- no ip ospf authentication key – Removes a previously assigned OSPF password.
- ip ospf message-digest-key - Enables OSPF MD5 authentication
- ip ospf authentication message-digest - Specifies the authentication type for an interface
- show ip ospf – Displays general information about OSPF routing process
- show ip ospf interface - Displays OSPF interface information

timers spf

Command Objective This command configures delay time and hold time between two consecutive SPF calculations.

The no form of the command resets the spf-delay and spf-holdtime to its default value.

Syntax **timers spf <spf-delay(0-65535)> <spf-holdtime(0-65535)>**

no timers spf

Parameter Description

- <spf-delay(0-65535)> - Configures the interval by which SPF calculation is delayed after a topology change reception. This value ranges between 0 and 65535 seconds.

- `<spf-holdtime(0-65535)>` - Configures the minimum time between two consecutive SPF calculations. This value ranges between 0 and 65535 seconds.

Mode OSPF Router Configuration Mode

Default

- spf-delay - 5 seconds
- spf-holdtime - 10 seconds

Example

```
Your Product(config-router)# timers spf 10 20
```

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `show ip ospf` – Displays general information about OSPF routing process

area - virtual-link key start-accept

Command Objective This command configures the time the router starts accepting packets that is created with the configured key id.

Syntax **area <area-id> virtual-link <router-id> key <Key-ID (0-255)> start-accept <DD-MON-YEAR,HH:MM>**

Parameter Description

- `<area-id>` - Specifies the area ID assigned to the transit area for the virtual link. The Transit Area is where the Virtual Link traverses. The area id value is either a decimal value or a valid IP address.
- `<router-id>` - Specifies the router ID of the virtual neighbor.
- `key <Key-ID (0-255)>` - Configures the secret key used to create the message digest appended to the OSPF packet. This value ranges between 0 and 255.
- `start-accept <DD-MON-YEAR,HH:MM>` - Configures the time when the router will start accepting packets that have been created with the configured key-id. This value is the sum of configured time and the system time at which the start-accept value is configured and is configured in 24- hours format.

  Note: For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30

Mode OSPF Router Configuration Mode

Note: This command executes only if ,

- Area is defined using the network command.
- Authentication key for Message Digest Authentication is configured for the specified area.

Example

```
Your Product(config-router)# area 1.1.1.1 virtual-link 12.1.1.1 key 5
```

```
start-accept 23-Jun-2013,19:18
```

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `network` - Defines the interfaces on which OSPF runs and the area ID
- `area - virtual-link` – Defines an OSPF virtual link and its related parameters
- `show ip ospf` – virtual –links - Displays parameters and the current state of OSPF virtual links
- `show ip ospf` – Displays general information about OSPF routing process

area - virtual-link key start-generate

Command Objective This command configures the time when the switch starts generating ospf packets with configured key id on the switch.

Syntax **area <area-id> virtual-link <router-id> key <Key-ID (0-255)> start-generate <DD-MON-YEAR,HH:MM>**

Parameter Description

- `<area-id>` - Specifies the area ID assigned to the transit area for the virtual link. The Transit Area is where the Virtual Link traverses. The area id value is either a decimal value or a valid IP address.
- `<router-id>` - Specifies the router ID of the virtual neighbor.
- `key <Key-ID (0-255)>` - Configures the secret key used to create the message digest appended to the OSPF packet. This value ranges between 0 and 255.
- `start-generate <DD-MON-YEAR,HH:MM>` - Configures the time when the switch will start generating ospf packets with the configured key id. This value is the sum of the configured time and the system time at which the start-generate value is configured. Start Generate Time value is configured in 24 hours format. Default value is set as current system time.

  Note: For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30

Mode OSPF Router Configuration Mode

Note: This command executes only if ,

- Area is defined using the network command.
- Authentication key for Message Digest Authentication is configured for the specified area.

Example

```
Your Product(config-router)# area 1.1.1.1 virtual-link 12.1.1.1 key 5
start-generate 23-Jun-2013,19:18
```

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `network` - Defines the interfaces on which OSPF runs and the area ID

- `area - virtual-link` – Defines an OSPF virtual link and its related parameters
- `show ip ospf` – virtual –links - Displays parameters and the current state of OSPF virtual links
- `show ip ospf` – Displays general information about OSPF routing process

area - virtual-link key stop-generate

Command Objective This command configures the time when the router stops generating packets with the configured key-id for packet generation in the switch.

Syntax **area <area-id> virtual-link <router-id> key <Key-ID (0-255)> stop-generate <DD-MON-YEAR,HH:MM>**

Parameter Description

- `<area-id>` - Specifies the area ID assigned to the transit area for the virtual link. The Transit Area is where the Virtual Link traverses. The area id value is either a decimal value or a valid IP address.
- `<router-id>` - Specifies the router ID of the virtual neighbor.
- `key <Key-ID (0-255)>` - Configures the secret key used to create the message digest appended to the OSPF packet. This value ranges between 0 and 255.
- `stop-generate <DD-MON-YEAR,HH:MM>` - Configures the time when the switch will stop generating ospf packets with the configured key id. Stop Generate value is configured in 24 hours format. Default value is set to the current system time.

Note: For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30

Mode OSPF Router Configuration Mode

Note: This command executes only if ,

- Area is defined using the network command.
- Authentication key for Message Digest Authentication is configured for the specified area.

Example

```
Your Product(config-router)# area 1.1.1.1 virtual-link 12.1.1.1 key 5 stop-
generate 23-Jun-2013,19:18
```

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `network` - Defines the interfaces on which OSPF runs and the area ID
- `area - virtual-link` – Defines an OSPF virtual link and its related parameters
- `show ip ospf` – virtual –links - Displays parameters and the current state of OSPF virtual links
- `show ip ospf` – Displays general information about OSPF routing process

area - virtual-link key stop-accept

Command Objective This command configures the time when the router stops accepting OSPF packets created by using the configured key-id.

Syntax **area <area-id> virtual-link <router-id> key <Key-ID (0-255)> stop-accept <DD-MON-YEAR,HH:MM>**

Parameter Description

- `<area-id>` - Specifies the area ID assigned to the transit area for the virtual link. The Transit Area is where the Virtual Link traverses. The area id value is either a decimal value or a valid IP address.
- `<router-id>` - Specifies the router ID of the virtual neighbor.
- `key <Key-ID (0-255)>` - Configures the secret key used to create the message digest appended to the OSPF packet. This value ranges between 0 and 255.
- `stop-accept<DD-MON-YEAR,HH:MM>` - Configures the time when the switch will stop accepting ospf packets with specified key id. Stop accept value is configured in 24-hours format

  Note: For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30

Mode OSPF Router Configuration Mode

Note: This command executes only if,

- Area is defined using the network command.
- Authentication key for Message Digest Authentication is configured for the specified area.

Example

```
Your Product(config-router)# area 1.1.1.1 virtual-link 12.1.1.1 key 5 stop-
accept 26-Jun-2013,19:18
```

Related Command(s)

- `router ospf` – Enables OSPF routing process
- `network` - Defines the interfaces on which OSPF runs and the area ID
- `area - virtual-link` – Defines an OSPF virtual link and its related parameters
- `show ip ospf - virtual -links` - Displays parameters and the current state of OSPF virtual links
- `show ip ospf` – Displays general information about OSPF routing process

31 VCM

VCM (Virtual Context Manager) enables IP protocol to work with multiple instance of switch. Supermicro switch defines two virtual contexts, one is the default context for in-band ports, another is mgmt context for out-of-band port (OOB or Management port). Each context has a individual VRF table (Virtual Routing and Forwarding) which is referred when an IP packet is received or transmitted by specified interface.

Traffic received on the OOB port is never switched or routed to any in-band port. Likewise, traffic received on any in-bind port is never forwarded or routes over the OOB port.

The virtual context is transparent to most switch applications such as Telnet, HTTP, DHCP…However, some applications have to specify the active routing context under different user scenarios such as

- ping
- traceroute
- tftp (including the file copy)
- coredump
- firmware upgrade
- send SYSLOG to logging server
- send SNMP trap
- as a SNTP client
- as a TACACS client

Those applications can go through either of default or mgmt routing context, and user can configure it and save it as a part of startup configuration.Please note those applications cannot work on both routing contexts simultaneously.
The list of CLI commands for VCM as follows:

- routing-context
- no routing-context
- show routing-context
- show switch
- show switch map info

routing-context

Command Objective This command configures the context in which application will route. Default context id is 0, named as “default”. Context name “mgmt” is used for OOB port with id 1. All incoming packet will be mapped to its context according to port index. But some application may route to OOB port or front port according to deployment and configuration. This command addresses the requirement for basic management.

Syntax **routing-context {firmware-upgrade | file-copy | coredump-put | syslog-client | snmp-trap |sntp-client | snmp-agentx | tacacs-client} vrf <vrf-name>**

Parameter Description

- `firmware-upgrade` – Firmware upgrade by CLI command
- `file-copy` – File, startup-config and debug-files copy by CLI command
- `coredump-put` – Coredump copy by CLI command
- `syslog-client` – Send log to SYSLOG server.
- `snmp-trap` – Send SNMP Trap and Inform to SNMP target.
- `sntp-client` – Send SNTP request to unicast server.
- `snmp-agentx` – Communicate with SNMP Master Agent.
- `tacacs-client` – Communicate with TACACS server.
- `vrf <vrf-name>` – Context name : “default” or “mgmt”

Mode Global Configuration Mode

Example

```
SMIS(config)# routing-context file-copy vrf default
```

Related Command(s)

- `show routing-context` – Display the the mapping of routing context
- `no routing-context` – Reset the context mapping to default

no routing-context

Command Objective This command resets the the mapping of routing contex to default

Syntax **no routing-context [{firmware-upgrade | file-copy | coredump-put | syslog-client | snmp-trap | sntp-client | snmp-agentx | tacacs-client }]**

Parameter Description

- `firmware-upgrade` – Default context is “mgmt”
- `file-copy` – Default context is “mgmt”
- `coredump-put` – Default context is “mgmt”
- `syslog-client` – Default context is “mgmt”.
- `snmp-trap` – Default context is “mgmt”
- `sntp-client` –Default context is “mgmt”
- `snmp-agentx` – Default context is “mgmt”
- `tacacs-client` –Default context is “mgmt”

Note: Reset all to default value if no application is specified

Mode Global Configuration Mode

Example SMIS# no routing-context firmware-upgrade

Related Command(s)

- `routing-context` – Configure the mapping of routing context

- `show routing-context` – Display the the mapping of routing context

show routing-context

Command Objective This command displays the mapping of routing context for applications

Syntax **show routing-context**

Mode Privileged EXEC Mode

Example

```
SMIS# show routing-context
                   Application       Context
                   -------------------     ---------------
                   firmware-upgrade   mgmt
                   file-copy          mgmt
                   coredump-put       mgmt
                   syslog-client      mgmt
                   snmp-trap          mgmt
                   sntp-client        mgmt
                   snmp-agentx        mgmt
                   tacacs-client        mgmt
```

Related Command(s) `routing-context` – Configure the mapping of routing context

show switch

Command Objective This command displays the virtual context table entries which are the information about the vlan interface mapping to different virtual routers.

Syntax **show switch [{brief | detail | interfaces}] [name]**

Parameter Description

- `brief` – Displays brief information about the virtual context table entries
- `detail` – Displays detailed information about the virtual context table entries
- `interfaces`**–** Displays interface related information about the virtual context table entries
- `name`**–** Displays information about the virtual context/switch name

Mode Privileged EXEC Mode

Example

```
SMIS# show switch interfaces
Interface map table
----------------------------
IfIndex  VcNum  Vc-Name                          LocalPortId
-------  -----  -------                          -----------
mgmt     1      mgmt                             0
```

```
vlan1     0       default                              0
```

Related Command(s) `show switch map info` – Displays the list of switch instances to which a physical or port channel interface is mapped.

show switch map info

Command Objective This commands displays the list of switch instances to which a physical or port channel interface is mapped

Syntax **show switch map info [interface <interface-type> <interface-id>]**

Parameter Description

- `<interface-type>` – Displays VCM status for the specified type of interface.

  The interface can be:

  - fastethernet
  - gigabitethernet
  - extreme-ethernet
  - qx-ethernet
- `<interface-id>` – Displays VCM status for the specified interface identifier.

Mode Privileged EXEC Mode

Example

```
SMIS# show switch map info inter extreme-ethernet 0/1
Port Context Mapping Info
=========================
-----------------------------------------------------------------
Port                : Ex0/1
Primary Context     : default
Secondary Contexts : None
-----------------------------------------------------------------
```

Related Command(s) `show switch` – Displays brief information about the virtual context table entries

32 BGP

The BGP (Border Gateway Protocol) is an inter-autonomous system routing protocol. An autonomous system is a network or group of networks under a common administration and with common routing policies. BGP is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems and is used between Internet service providers (ISP). BGP is often the protocol used between gateway hosts on the Internet. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen.

Hosts using BGP communicate using the Transmission Control Protocol (TCP) and send updated router table information only when one host has detected a change. BGP is commonly used within and between Internet Service Providers (ISPs).

The list of CLI commands for the configuration of BGP is as follows:

- router bgp
- ip bgp dampening
- bgp dampening
- ip bgp overlap-policy
- default-information originate
- ip bgp synchronization
- synchronization
- bgp router-id
- bgp default local-preference
- bgp default ipv4-unicast
- neighbor - remote-as
- neighbor - activate
- neighbor - ebgp-multihop
- neighbor - next-hop-self
- neighbor - interval
- neighbor - timers
- neighbor - shutdown
- neighbor - update-source
- neighbor - gateway
- neighbor - network-address
- neighbor - default-originate
- neighbor - send-community
- neighbor - capability
- bgp nonbgproute-advt
- redistribute
- import route
- bgp always-compare-med
- default-metric

- bgp med
- bgp local-preference
- bgp update-filter
- aggreate-address index
- bgp cluster-id
- bgp client-to-client reflection
- neighbor - route-reflector-client
- bgp comm-route
- bgp comm-filter
- bgp comm-policy
- bgp ecomm-route
- bgp ecomm-filter
- bgp ecomm-policy
- bgp confederation identifier
- bgp confederation peers
- bgp bestpath med confed
- neighbor - password
- address-family
- bgp graceful-restart
- bgp update-delay
- restart-support
- restart-reason
- distribute-list route-map
- distance
- clear ip bgp
- do shutdown ip bgp
- debug ip bgp
- show bgp-version
- show ip bgp
- show ip bgp restart mode
- show ip bgp EndOfRIBMarkerStatus
- show ip bgp restartreason
- show ip bgp restartexitreason
- show ip bgp restartsupport
- show ip bgp restartstatus
- show ip bgp extcommunity - routes
- show ip bgp summary
- show ip bgp filters
- show ip bgp aggregate
- show ip bgp med
- show ip bgp dampening
- show ip bgp local-pref
- show ip bgp timers

- show ip bgp info
- show ip bgp rfl info
- show ip bgp confed info
- show ip bgp community
- show ip bgp extcommunity
- neighbor - maximum-prefix
- neighbor - connect-retry-count
- neighbor - allow-autostop
- neighbor - damp-peer-oscillations
- neighbor delay-open
- bgp trap
- neighbor - peer group
- neighbor <ip-address> peer-group
- neighbor - routemap
- neighbor - transport connection-mode
- nexthop processing-interval
- bgp redistribute internal
- show ip bgp peer-group
- redistribute ospf
- neighbor - local-as
- maximum-paths
- tcp-ao mkt key-id – receive-key-id
- neighbor - tcp-ao
- neighbor - tcp-ao
- neighbor - tcp-ao mkt
- neighbor - tcp-ao - start-accept
- neighbor - tcp-ao - stop-accept
- neighbor - tcp-ao - start-generate
- neighbor - tcp-ao - stop-generate
- show ip bgp - tcp-ao neighbor
- show ip bgp - tcp-ao mkt summary
- ip bgp four-byte-asn
- bgp asnotation dot

router bgp

Command Objective This command configures the AS (Autonomous System) number of the BGP Speaker and enters into BGP router configuration mode. The no form of the command configures the AS number of the BGP Speaker to its default value.

Note: If this value is already configured to a non-zero value, it must be reset to zero (using no form of the command) before reconfiguring.

Syntax **router bgp <AS no> [vrf <vrf-name>]**

no router bgp [vrf <string (32)>]

Parameter Description

- `vrf <vrf-name>` - Configures the AS (Autonomous System) number of the BGP Speaker for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

  Note: When VRF is not specified the configurations are done for the default VRF.

- `<AS no>` - Configures the AS (Autonomous System) number of the BGP Speaker and enters into BGP router configuration mode. The AS number identifies the BGP router to other routers and tags the routing information passed along This command also allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems. This value ranges between 1 and 4294967295 or 0.1 to 65535.65535.

  Notes:

  - When four-byte-asn is enabled, this value ranges between 1 and 4294967295or between 0.1 and 65535.65535
  - When four-byte-asn is disabled, this value ranges between 1 and 65535. or between 0.1 and 0.65535
  - When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.65535

Mode Global Configuration Mode

Default 0

Example Your Product(config)# router bgp 100

Related Command(s)

- `as-num` - Sets the autonomous number for the router.
- `ip address` - Sets the IP address for an interface
- `router-id` - Sets the router ID's address for the router
- `ip bgp dampening` – Configures the Dampening Parameters
- `ip bgp overlap-policy` – Configures the Overlap Route policy for the BGP Speaker
- `ip bgp synchronization / synchronization` – Enables synchronization between BGP and IGP
- `bgp router-id` – Configures the BGP Identifier of the BGP Speaker
- `bgp default local-preference` – Configures the Default Local Preference value
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer
- `neighbor - activate` – Enables default capabilities for the peer and restarts the connnection to the peer if capabilities negotiated change
- `neighbor - ebgp-multihop` – Enables BGP to establish connection with external peers

- `neighbor - next-hop-self` – Enables BGP to send itself as the next hop for advertised routes
- `neighbor - interval` – Configures neighbor interval
- `neighbor - timers` – Configures neighbor KeepAlive Time and Hold Time Intervals
- `neighbor - shutdown` – Disables the Peer session
- `neighbor - update-source` - Configures the source-address for routing updates and for TCP connection establishment with a peer
- `neighbor - gateway` - Configures gateway router's address that will be used as nexthop in the routes advertised to the peer
- `neighbor - network-address` - Configures peer's remote IPv6 network address for IPv4 peer and peer's remote IPv4 network address for IPv6 peer
- `neighbor - default` - originate - Enables advertisement of the default route to the peer
- `neighbor - send-community` – Enables advertisement of community attributes to (standard/extended) to peer
- `neighbor - capability` - Enables the specific BGP capability to be advertised and received from the peer
- `neighbor - delay open` - Configures a delay in sending the first OPEN message to the BGP peer for a specific time period.
- `neighbor - damp-peer-oscillations` - Enables the damp peer oscillation option
- `neighbor - maximum prefix` - Configures the maximum number of peers supported by BGP
- `neighbor - allow-autostop` - Enables the auto stop option to stop the BGP peer and BGP connection automatically
- `neighbor - connect-retrycount` - Sets the retry count for the BGP peer
- `neighbor - transport connection-mode` - Configures the BGP Peer Transport Connection status as active or passive.
- `bgp nonbgproute-advt` – Controls the advertisement of Non-BGP routes
- `no ip bgp overlap-policy` – Resets the Overlap route policy to default
- `redistribute` – Configures the protocol from which the routes have to be redistributed into BGP.
- `bgp always-compare-med` – Enables the comparison of med for routes received from different autonomous system.
- `default-metric` – Configures the Default IGP Metric value
- `bgp med` – Configures an entry in MED Table
- `bgp local-preference` – Configures an entry in Local Preference Table
- `bgp update-filter` – Configures an entry in Update Filter Table
- `aggregate-address index` – Configures an entry in Aggregate Table
- `bgp cluster-id` – Configures the Cluster ID for Route Reflector.
- `bgp client-to-client reflection` – Configures the Route Reflector to support route reflection to Client Peers
- `neighbor - route-reflector-client` – Configures the Peer as Client of the Route Reflector
- `bgp comm-route` – Configures an entry in additive or delete community table
- `bgp comm-filter` – Allows/filters the community attribute while receiving or advertising
- `bgp comm-policy` – Configures the community attribute advertisement policy for specific destination
- `bgp ecomm-route` – Configures an entry in additive or delete ext community table

- `bgp ecomm-filter` – Allows/filters the ext community attribute while receiving or advertising
- `bgp ecomm-policy` – Configures the extended community attribute advertisement policy for specific destination
- `bgp confederation identifier` – Specifies the BGP confederation identifie.
- `bgp confederation peers` – Configures the ASs that belongs to the confederation
- `bgp bestpath med confed` – Enables MED comparison among paths learnt from confed peers
- `neighbor - password` – Configures the password for TCP-MD5 authentication with peer.
- `bgp graceful-restart` - Enables the graceful restart capability.
- `bgp update-delay` - Configures the selection deferral time interval
- `restart-support` - Enables the graceful restart support
- `restart-reason` - Configures the reason for BGP graceful restart
- `distribute-list route-map` - Enables route map filtering for inbound or outbound route
- `distance` - Enables the administrative distance of the routing protocol and sets the administrative distance value
- `debug ip bgp` – Configures the Trace levels.
- `bgp trap` – Enables/disables the bgp trap notification
- `show bgp-version` – Displays the BGP Version information
- `show ip bgp` – Displays the BGP related information
- `show ip bgp community` - routes– Displays routes that belong to specified BGP communities
- `show ip bgp extcommunity - routes` – Displays routes that belong to specified BGP extended-communities
- `show ip bgp summary` – Displays the status of all BGP4 connections
- `show ip bgp filters` – Displays the contents of filter table
- `show ip bgp aggregate` – Displays the contents of aggregate table
- `show ip bgp med` – Displays the contents of MED table
- `show ip bgp dampening` – Displays the contents of dampening table
- `show ip bgp local-pref` – Displays the contents of local preference table
- `show ip bgp timers` – Displays the value of BGP timers
- `show ip bgp info` – Displays the general information about BGP protocol
- `show ip bgp rfl info` – Displays information about RFL feature
- `show ip bgp confed info` – Displays information about confederation feature
- `show ip bgp community` – Displays the contents of community tables
- `show ip bgp extcommunity` – Displays the contents of ext-community tables
- `nexthop processing-interval` - configures the interval at which next hops are monitored for reachablity
- `redistribute ospf` - Configures the OSPF protocol from which the routes are redistributed into BGP
- `show ip bgp - tcp-ao mkt summary` - Displays the BGPrelated TCP-AO MKT information
- `tcp-ao mkt key-id - receive-key-id` - Creates a TCP-AO MKT in the BGP instance
- `neighbor - tcp-ao mkt` - Associates a TCP-AO MKT to the BGP peer
- `neighbor - tcp-ao` – sets BGP peer TCP-AO configurations
- `ip bgp four-byte-asn` - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system

- `bgp asnotation dot` - Changes the output format of BGP ASNs from asplain to asdot notation

ip bgp dampening

Command Objective This command configures the dampening parameters, changes various BGP route dampening factors and also enables bgp dampening in the system or the specified VRF instance when none of the RFD parameters are specified.

The no form of the command disables the dampening feature in the system or in the specified VRF instance. When the RFD parameter options are not specified in the no form of the command it disables the dampening features and does not reset the values related to RFD.But when the RFD parameter options are specified in the no form of the command, the parameters are reset to its default values.

Note: The RFD parameters configured can be viewed using the `show ip bgp dampening`command even when RFD is disabled.

Syntax **ip bgp dampening [vrf <vrf-name>] [HalfLife-Time <integer(600-2700)>] [Reuse-Value <integer(100-1999)>] [Suppress-Value <integer(2000-3999)>] [Max-Suppress-Time <integer(1800-10800)>] [-s Decay-Granularity <integer(1-10800)>] [Reuse-Granularity <integer(15-10800)>] [Reuse-Array-Size <integer(256-65535)>]**

no ip bgp dampening [vrf <vrf-name>] [HalfLife-Time [Reuse-Value [Suppress-Value [Max-Suppress-Time]]]] [-s Decay-Granularity [Reuse-Granularity [Reuse-Array-Size]]]

Parameter Description

- `vrf <vrf-name>` - Configures the dampening parameters for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

  Note: When VRF is not specified the configurations are done for the default.

- `HalfLife-Time<integer(600-2700)>` - Configures the Time (in seconds) after which a penalty is decreased by half after the half-life period. Once a route has been assigned a penalty, the penalty is decreased for every 5 seconds. BGP's route flap damping algorithm calculates penalty for each routes. This penalty increases by a fixed value when a flap occurs, and decreases exponentially when the route is stable. This value ranges between 600 and 2700.
- `Reuse Value integer(100-1999)>` - Configures the reuse value. If the penalty for a flapping route fallsbelow this value, the route is re-used. The unsuppressing of routes occurs at 10-second increments. This value ranges between 100 and 1999.

  Note: Reuse value can be configured only if the HalfLife Time value is set.

- `Suppress Value<integer(2000-3999)>` - Configures the suppress value. The route is suppressed if the penalty associated with the route exceeds this value. This value ranges between 2000 and 3999.

  Note: Suppress value can be configured only if the HalfLife Time and Reuse value are set.

- `Max-Suppress Time<integer(1800-10800)` - Configures the maximum time (in seconds) a route can be suppressed. This value ranges between 1800 and 10800. Max-Suppress Time can be configured only if the HalfLife Time, Reuse Value and Suppress Value are set.
- `-s Decay Granularity<integer(1-10800)>` - Configures the time granularity in seconds used to perform all decay computations. This value ranges between 1 and 10800.
- `Reuse Granularity<integer(15-10800)>` - Configures the time interval between evaluations of the reuse-lists. Each reuse lists corresponds to an additional time increment. This value ranges between 15 and 10800.
- `Reuse Array Size<integer(256-65535)>` - Configures the size of reuse index arrays. This size determines the accuracy with which suppressed routes can be placed within the set of reuse lists when suppressed for a long time. This value ranges between 256 and 65535.

  Note: This command executes only if BGP Speaker Local AS number is configured.

Mode Global Configuration Mode

Default

- HalfLife-Time - 900 seconds
- Reuse Value - 750
- Suppress Value - 2000
- Max-Suppress Time - 3600 seconds
- Decay Granularity - 1 second
- Reuse Granularity - 15
- Reuse Array Size - 1024

Example

```
Your Product(config)# ip bgp dampening HalfLife-Time 1000 reuse-Value 1998
Suppress-Value 2000 -s Decay-Granularity 1 reuse-Granularity 135 reuse-
Array-Size 257
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `bgp dampening` – Sets the BGP dampening parameters.
- `show ip bgp dampening` – Displays the contents of dampening table.

bgp dampening

Command Objective This command configures the Dampening parameters or changes various BGP route dampening factors and. The arguments half-life, reuse, suppress, and max-suppress-time are position-dependent hence, if any of them are used, they must all be specified.

The no form of the command disables the bgp dampening feature and does not reset the other configured RFD parameters.

Note: The RFD parameters configured can be viewed via "show ip bgp dampening" even when RFD is disabled.

This command is a complete standardized implementation of the existing command and operates similar to that of the command ip bgp dampening.

Syntax **bgp dampening <HalfLife-Time(600-2700)> <Reuse-Value(100-10800)> <Suppress-Value(2000-3999)> <Max-Suppress-Time(1800-10800)>**

no bgp dampening

Parameter Description

- `<HalfLife-Time (600-2700)>` - Configures the Time (in seconds) after which a penalty is decreased by half. Once a route has been assigned a penalty, the penalty is decreased for every 5 seconds. BGP's route flap damping algorithm calculates penalty for each routes. This penalty increases by a fixed value when a flap occurs, and decreases exponentially when the route is stable. This value ranges between 600 and 2700.
- `<Reuse Value (100-10800)>` - Configures the reuse value. If the penalty for a flapping route falls below this value, the route is re-used. The unsuppressing of routes occurs at 10-second increments. This value ranges between 100 and 10800.

  Note: Reuse value can be configured only if the HalfLife Time value is set.

- `<Suppress Value (2000-3999)>` - Configures the suppress value. The route is suppressed if the penalty associated with the route exceeds this value. This value ranges between 2000 and 3999.

  Note: Suppress value can be configured only if the HalfLife Time and Reuse value are set.

- `<Max-Suppress Time (1800-10800)>` - Configures the maximum time (in seconds) a route can be suppressed. This value ranges between 1800 and 10800.

  Note: Max-Suppress Time can be configured only if the HalfLife Time, Reuse Value and Suppress Value are set.

Mode Global Configuration Mode

Default

- HalfLife-Time - 900 seconds
- Reuse Value - 750
- Suppress Value - 2000
- Max-Suppress Time - 3600 seconds

Example

```
Your Product(config-router)# bgp dampening 1000 300 2000 5000
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `ip bgp dampening` – Sets the BGP dampening parameters

- `show ip bgp dampening` – Displays the contents of dampening table.

ip bgp overlap-policy

Command Objective This command configures the BGP speaker's policy for handling the overlapping routes.

The no form of the command resets the Overlap route policy to its default value. By default, both less and more specific routes are installed.

Syntax **ip bgp overlap-policy [vrf <vrf-name>] {more-specific|less-specific|both}**

no ip bgp overlap-policy [vrf <vrf-name>]

Parameter Description

- `vrf <vrf-name>` - Configures the BGP speaker's policy for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32
- `more-specific` - Configures the Overlap Policy for BGP speaker as more-specific. This implies that when an overlapping route is received more-specific routes are installed in the RIB tree.
- `less-specific` - Configures the Overlap Policy for BGP speaker as less-specific. This implies that when an overlapping route is received less-specific routes are installed in the RIB tree
- `both` - Configures the Overlap Policy for BGP speaker as both. This implies that when an overlapping route is received both more-specific and less-specific routes are installed in the RIB tree

Mode Global Configuration Mode

Default both

Note: This command executes only if BGP Speaker Local AS number is configured and BGP Administrative status is DOWN

Example

```
Your Product(config)# ip bgp overlap-policy more-specific
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker
- `do shutdown ip bgp` – Sets the BGP Speaker Global Admin status DOWN
- `show ip bgp info` – Displays the general information about BGP protocol

default-information originate

Command Objective This command enables and controls redistribution of default routes of a protocol or network into the BGP and advertisement of the default route (0.0.0.0/0). The default route advertisement is possible only if the default route is present in the IP FDB or it is received from any peers.

The no form of the command disables redistribution and advertisement of the default route. The default routes are not redistributed into BGP.

Syntax **default-information originate [vrf <vrf-name>]**

no default-information originate [vrf <vrf-name>]

Parameter Description `vrf <vrf-name>` - Enables and controls redistribution and advertisement of default routes for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32

Mode Global Configuration Mode

Default Default Information Originate is disabled.

Note: This command executes only if BGP Speaker local AS number is configured.

Example

```
Your Product(config)# default-information originate
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp info` - Displays the general information about BGP protocol.

ip bgp synchronization

Command Objective This command enables synchronization between Border Gateway Protocol (BGP) and Interior Gateway Protocol (IGP). BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP.

This command allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems.

The no form of the command disables synchronization between BGP and IGP.

Syntax **ip bgp synchronization [vrf <vrf-name>]**

no ip bgp synchronization [vrf <vrf-name>]

Parameter Description `vrf <vrf-name>` - Enables synchronization between BGP and IGP for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Global Configuration Mode

Default Synchronization between BGP and IGP is disabled.

Note: This command executes only if BGP Speaker local AS number is configured.

Example

```
Your Product(config)# ip bgp synchronization
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `synchronization` - Enables synchronization between Border Gateway Protocol (BGP) and Interior Gateway Protocol (IGP)
- `show ip bgp info` - Displays the general information about BGP protocol.

synchronization

Command Objective This command enables synchronization between Border Gateway Protocol (BGP) and Interior Gateway Protocol (IGP). BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP. This command allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems. The no form of the command disables synchronization between BGP and IGP.

This command is a complete standardized implementation of the existing command and operates similar to that of the command ip bgp synchronization.

Syntax **synchronization**

no synchronization

Parameter Description `vrf <vrf-name>` - Enables synchronization between BGP and IGP for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode BGP Router Configuration Mode

Default The synchronization between the BGP and IGP is disabled.

Example

```
Your Product(config-router)# synchronization
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `ip bgp synchronization` - Enables synchronization between Border Gateway Protocol (BGP) and Interior Gateway Protocol (IGP)
- `show ip bgp info` - Displays the general information about BGP protocol.

bgp router-id

Command Objective This command configures fixed BGP router identifier for a BGP-speaking router. If loopback interface exists, the router ID is set to the highest address for loopback interface otherwise it is set to the highest ip configured on the ip interfaces.. Peering sessions will be reset if the router ID is changed. BGP router id is a unique number associated with the BGP speaker. This router-id is advertised to other peers and identifies the BGP speaker uniquely. Administrator can set the router-id of BGP to any value. If router-id is changed, then all the active peer sessions will go DOWN and will be re-started with the new configured router-id.

The no form of the command resets the BGP Identifier of the BGP Speaker to its default value.

Syntax **bgp router-id <bgp router id (ip-address)>**

no bgp router-id

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default The highest interface address is used as the router id.

Example

```
Your Product(config-router)# bgp router-id 10.0.0.1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp` – Displays the BGP related information
- `show ip bgp summary` – Displays the status of all BGP4 connections.
- `address-family` - Enters the router into the address-family router configuration mode

bgp default local-preference

Command Objective This command configures the default local preference value that is to be sent in updates to internal peers. The preference is sent to all routers and access servers in the local autonomous system. This value ranges between 1 and 2147483647.

The no form of the command resets the default local preference to its default value.

Syntax **bgp default local-preference <Local Pref Value>**

no bgp default local-preference

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 100

Example

```
Your Product(config-router)# bgp default local-preference 150
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp info` – Displays the general information about BGP protoco.
- `address-family` - Enters the router into the address-family router configuration mode

bgp default ipv4-unicast

Command Objective This command enables default routing to IPv4-unicast. By default the MP (Multi

Protocol) IPv4 Unicast Address Family Capability is negotiated for a peer, when the peer is created. It will not be negotiated for a peer if the default routing configuration is reset. This command affects the negotiation of the MP IPv4 Unicast Address Family Capability for the peers newly created and will not affect the MP IPV4 Unicast negotiation status of the already existing peer.

The no form of the command disables default routing to IPv4 unicast which implies that if a neighbor is created, then IPv4 unicast capability will not be negotiated unless IPv4 unicast capability is explicitly configured for that neighbor.

Syntax **bgp default ipv4-unicast**

no bgp default ipv4-unicast

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default The default routing to IPv4-unicast is enabled.

Example

```
Your Product(config-router)# bgp default ipv4-unicast
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode

neighbor - remote-as

Command Objective This command creates a peer and initiates the connection to the peer and adds an entry to the BGP or multiprotocol BGP neighbor table. This specifies a neighbor with an autonomous system number that identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered as external. By default, neighbors that are defined using this command in router configuration mode exchange only unicast address prefixes.

The administrator can create a peer and set the Peer AS number with this command. The configured Peer AS number is compared with the AS number received in the open message and a peer session is initiated only if both the AS numbers match.

The no form of the command disables the peer session and deletes the peer information.

Syntax **neighbor <ip-address / peer-group-name> remote-as <AS no> [allow-autostart [idlehold-time <integer(1-65535)>]]**

no neighbor <random_str> [remote-as <AS no> [allow-autostart]]

Parameter Description

- `<ip-address> / <random_str>` - Configures the BGP peer's remote IP address.
- `<peer-group-name>` - Configures a BGP peer group by using the peer- group-name argument. The

members of the peer group will inherit the characteristic configured with this command.

Note: The peer group has been configured prior to setting the remote-as number for the peer-group.

- `remote-as<AS no(1-65535)>` - Configures the Autonomous system number of the peer. This value ranges between 1 and 4294967295 or 0.1 to 65535.65535.

  Notes:

  - When four-byte-asn is enabled, this value ranges between 1 and 4294967295 or between 0.1 and 65535.65535
  - When four-byte-asn is disabled, this value ranges between 1 and 65535. or between 0.1 and 0.65535
  - When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.65535.
- `allow-autostart` - Starts BGP session with the associated peer automatically. The peer session is automatically started in the IDLE state, after a BGP Peer session is brought down either by Autostop or through reception of invalid BGP message. The BGP session is automatically started after an interval specified by idle hold timer.
- `idlehold-time <integer(1-65535)>` - Configures the idle hold time. This specifies the length of time the BGP peer is held in the Idle state prior to the next automatic restart. This value ranges between 1 and 65535.

  Notes:

  - The IdleHoldTime can be configured only when the allow-autostart is enabled
  - After each dampening, the value of the Idle Hold Time is doubled consecutively

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Example `Your Product(config-router)# neighbor 23.45.0.1 remote-as 66`

Default

- allow-autostart is disabled
- idlehold-time-60 seconds

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - activate` – Enables default capabilities for the peer and restarts the connnection to the peer if capabilities negotiated change
- `neighbor - peer-group` – Creates a peer group.
- `neighbor - ebgp-multihop` – Enables BGP to establish connection with external peers
- `neighbor - next-hop-self` – Enables BGP to send itself as the next hop for advertised routes.
- `neighbor - interval` – Configures neighbor interval

- `neighbor - timers`– Configures neighbor KeepAlive Time and Hold Time Intervals.
- `neighbor - shutdown` – Disables the Peer session
- `neighbor - update-source` - Configures the source-address for routing updates and for TCP connection establishment with a peer.
- `neighbor – gateway` - Configures gateway router's address that will be used as nexthop in the routes advertised to the peer.
- `neighbor - network-address` - Configures peer's remote IPv6 network address for IPv4 peer and peer's remote IPv4 network address for IPv6 peer.
- `neighbor - default-originate` - Enables advertisement of the default route to the peer.
- `neighbor - send-community` – Enables advertisement of community attributes to (standard/extended) to peer.
- `neighbor - capability` - Enables the specific BGP capability to be advertised and received from the peer.
- `neighbor - password` – Configures the password for TCP-MD5 authentication with peer.
- `neighbor delay open` –Configures a delay in sending the first OPEN message to the BGP peer for a specific time period.
- `neighbor damp-peer-oscillations` - Enables the damp peer oscillation option.
- `neighbor maximum prefix` - Configures the maximum number of peers supported by BGP
- `neighbor - allow-autostop` - Enables the auto stop option to stop the BGP peer and BGP connection automatically.
- `neighbor – transport connection-mode` - Configures the BGP Peer Transport Connection status as active or passive
- `neighbor <ip-address> peer-group` – Adds the neighbor as a member of the specified peer group.
- `neighbor – connect-retrycount` - Sets the retry count for the BGP peer
- `show ip bgp summary` - Displays the status of all BGP4 connections.
- `show ip bgp` - Displays the BGP related information.
- `show ip bgp restart mode` - Displays the restart mode of the BGP router and neighbors.
- `show ip bgp EndOfRIBMarkerStatus` - Displays the End_Of_RIB marker status of the BGP router and neighbors.
- `show ip bgp restartexitreason` - Displays the restart exit reason of the BGP.
- `show ip bgp restartsupport` - Displays the restart support of the BGP.
- `show ip bgp restartstatus` –Displays the restart status of the BGP.
- `show ip bgp timers` - Displays the value of BGP timers.
- `show ip bgp info` – Displays the general information about BGP protocol.
- `show ip bgp peer-group` – Displays information abouty the peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `neighbot – tcp-ao` - Sets BGP peer TCP-AO configurations.
- `neighbot – tcp-ao mkt` –Associates a TCP-AO MKT to the BGP peer.
- `neighbor tcp-ao mkt - start-accept` - Configures the start accept value for the MKT for the specified BGP peer.
- `neighbor tcp-ao mkt - stop-accept` - Configures the stop accept value for the MKT for the specified BGP peer.

- neighbor tcp-ao mkt - start-generate - Configures the start generate value for the MKT for the specified BGP peer.
- neighbor tcp-ao mkt - stop-generate - Configures the stop generate value for the MKT for the specified BGP peer.
- ip bgp four-byte-asn - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system.
- bgp asnotation dot - Changes the output format of BGP ASNs from asplain to asdot notation
- show ip bgp - tcp-ao neighbor - Displays the TCP-AO information for the specified BGP peer.

neighbor - activate

Command Objective This command enables the default capabilities associated with the address-family of the peer. If the capabilities negotiated with the peer are modified due to enabling of the default capabilities, the connection with the peer will be restarted. The default local capabilities for IPv4 peer are "IPv4 Unicast" and "route Refresh". The default local capabilities for IPv6 peer are "IPv6 Unicast" and "Route Refresh".

The no form of the command resets the peer after disabling the default capabilities associated with the address-family of the peer.

Syntax **neighbor <ip-address|peer-group-name> activate**

no neighbor <ip-address> activate

Parameter Description

- <ip-address> - Enables default capabilities for the specified BGP peer's IP address.
- <peer-group-name> - Enables default capabilities for the specified BGP peer group.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 activate
```

Related Command(s)

- router bgp – Sets the AS number of the BGP Speaker.
- neighbor - remote-as – Creates a Peer and initiates the connection to the peer.
- neighbor - peer-group – Creates a peer group.
- show ip bgp – Displays the BGP related information.
- show ip bgp info – Displays the general information about BGP protocol.
- show ip bgp peer-group – Displays information abouty the peer group.
- address-family - Enters the router into the address-family router configuration mode.

neighbor – ebgp-multihop

Command Objective This command enables BGP to establish connection with external peers residing on networks that are not directly connected.

By default, external BGP peers need to be directly connected. If external BGP peer are not connected directly, then ebgp-multihop is enabled to initiate the connection with that external peer. If ebgp-multihop is disabled and external BGP peers are indirectly connected, then BGP peer session will not be established.

The no form of the command disables the peer EBGP-Multihop feature.

Syntax **neighbor <ip-address | peer-group-name> ebgp-multihop ebgp-multihop [ttl]**

no neighbor <ip-address | peer-group-name> ebgp-multihop

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP-speaking neighbor.
- `<peer-group-name>` - Configures a BGP peer group by using the peer- group-name argument. The members of the peer group will inherit the characteristic configured with this command.
- `ttl` - Configures the maximum hop limit that is allowed for indirect BGP session. This value ranges between 1 and 255.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default EBGP Multihop is disabled.
ttl-1

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 ebgp-multihop ttl 20
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `show ip bgp info` – Displays the general information about BGP protocol.
- `show ip bgp peer-group` – Displays information abouty the peer group.
- `address-family` - Enters the router into the address-family router configuration mode.

neighbor – next-hop-self

Command Objective This command configures the router as the next hop for BGP-speaking neighbor or peer group and enables BGP to send itself as the next hop for advertised routes. Administrator uses this command to make BGP speaker fill its address when advertising routes to the BGP peer. This command is useful in non-meshed networks where BGP neighbors may not have direct access to all other neighbors on the same IP subnet.

The no form of the command resets the peer nexthop-self status to default. The next hop will be generated based on the IP address of the destination and the present next hop in the route information.

Syntax **neighbor <ip-address | peer-group-name> next-hop-self**
no neighbor <ip-address | peer-group-name> next-hop-self

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<peer-group-name>` - Configures a BGP peer group by using the peer- group-name argument. The members of the peer group will inherit the characteristic configured with this command.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 next-hop-self
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `show ip bgp info` – Displays the general information about BGP protocol.
- `show ip bgp peer-group` – Displays information abouty the peer group.
- `address-family` - Enters the router into the address-family router configuration mode.

neighbor – interval

Command Objective This command configures the minimum neighbor interval between the sending of BGP routing updates.

The no form of the command configures the neighbor interval to its default value.

Syntax **neighbor <ip-address | peer-group-name> {advertisement-interval <seconds(1-65535)> | as-origination-interval <seconds(1-65535)> | connect-retry-interval<seconds(1-65535)>}**

no neighbor <ip-address | peer-group-name> {advertisement-interval | as-origination-interval | connect-retry-interval}

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.

- `<peer-group-name>` - Configures a BGP peer group by using the peer- group-name argument. The members of the peer group will inherit the characteristic configured with this command.
- `advertisement-interval<seconds(1-65535)>` - Configures the advertisement interval which is the time-interval (in seconds) for spacing advertisement of successive external route-updates to the same destination. This value ranges between 1 and 65535.
- `as-origination-interval<seconds(1-65535)>` - Configures the AS origination interval which is the time-interval (in seconds) for spacing successive route-updates originating within the same AS. This value ranges between 1 and 65535.
- `connect-retry-interval<seconds(1-65535)>` - Configures the time interval (in seconds) after which a transport connection with peer is re-initiated. This value ranges between 1 and 65535.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default advertisement-interval - 30 seconds for EBGP Connections, 5 seconds for IBGP Connections

as-origination-interval - 15 seconds

connect-retry-interval - 30 seconds

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 advertisement-interval 45
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `show ip bgp` – Displays the BGP related information.
- `show ip bgp timers` – Displays the value of BGP timers.
- `show ip bgp info` – Displays the general information about BGP protocol.
- `address-family` - Enters the router into the address-family router configuration mode.

neighbor – timers

Command Objective This command configures neighbor KeepAlive Time and Hold Time Intervals and sets the timers for a specific BGP peer or peer group.

The no form of the command configures the neighbor KeepAlive Time and Hold Time Intervals to its default value.

Syntax **neighbor <ip-address | peer-group-name> timers {keepalive < (1-21845) seconds> | holdtime < (3-65535) seconds> | delayopentime <(0-65535)seconds>}**

no neighbor <ip-address | peer-group-name> timers {keepalive | holdtime|

delayopentime}

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<peer-group-name>` - Configures a BGP peer group by using the peer- group-name argument. The members of the peer group will inherit the characteristic configured with this command.
- `keepalive < (1-21845) seconds>` - Configures the keep alive interval (in seconds) or frequency with with keep alive messages are sent to its peer for the peer session. The keep-alive value must always be less than the configured hold-time value. The value ranges between 1 and 21845.
- `holdtime < (3-65535) seconds>` - Configures thehold-time interval (in seconds) for the peer, which is sent in the OPEN message to the peer. This is the time interval in seconds for the Hold Time configured for BGP speaker with the peer. The system declares a peer dead, after ensuring that keep alive message is not received within this time period from the peer. This value ranges between 3 and 65535 seconds.
- `delayopentime <(0-65535)seconds>` - Configures the delay open time which is the amount of time that the BGP peer should delay in sending the OPEN message to the remote peer. This value ranges between 0 and 65535.

  Note: The value 0 implies that the BGP Peer can send an OPEN message without any delay to its neighbor.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default keepalive - 30 seconds

holdtime - 90 seconds

Delayopentime - 0 seconds

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 timers keepalive 40
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `show ip bgp` – Displays the BGP related information.
- `show ip bgp timers` – Displays the value of BGP timers.
- `show ip bgp info` – Displays the general information about BGP protocol.
- `address-family` - Enters the router into the address-family router configuration mode.

neighbor – shutdown

Command Objective This command disables the Peer session and terminates any active session for the specified neighbor or peer group and removes all associated routing information. In the case of a peer group, a large number of peering sessions could be terminated suddenly.

The no form of the command enables the Peer session for the specified neighbor.

Syntax **neighbor <ip-address | peer-group-name> shutdown**

no neighbor <ip-address | peer-group-name> shutdown

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<peer-group-name>` - Configures a BGP peer group by using the peer- group-name argument. The members of the peer group will inherit the characteristic configured with this command.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode
Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 shutdown
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `show ip bgp` – Displays the BGP related information.
- `show ip bgp peer-group` – Displays information abouty the peer group.
- `address-family` - Enters the router into the address-family router configuration mode.

neighbor – update-source

Command Objective This command configures the source-address for routing updates and allows BGP sessions to use any operational interface for TCP connection establishment with a peer.

The no form of the command disables configured source-address for routing updates and for TCP connection establishment with a peer.

Syntax **neighbor < ip-address > update-source <random_str>**

no neighbor < ip-address > update-source <random_str>

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<random_str>` - Configures the IP address to be used as source for routing updates and TCP

connection establishment. This IP address can be any interface address.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default The source address is set as 0.0.0.0, and the TCP fills the source address of the TCP session.

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 update-source 40.0.0.1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor` - remote-as – Creates a Peer and initiates the connection to the peer.
- `show ip bgp` – Displays the BGP related information.
- `address-family` - Enters the router into the address-family router configuration mode.

neighbor – gateway

Command Objective This command configures gateway router's address that will be used as nexthop in the routes advertised to the peer. This ensures that the traffic coming from this peer is routed through the gateway configured.

The no form of the command resets the configured gateway router's address.

Syntax **neighbor < ip-address > gateway <random_str>**

no neighbor < ip-address > gateway

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<random_str>` - Configures the IP address of the gateway to be used as next hop.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 gateway 10.0.0.1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `show ip bgp` – Displays the BGP related information.
- `address-family` - Enters the router into the address-family router configuration mode.

neighbor – network-address

Command Objective This command configures peer's remote IPv6 network address for IPv4 peer and peer's remote IPv4 network address for IPv6 peer.

The peer's network address carries the IPv6 network address if the peer's remote-address is an IPv4 address. The peer's network address carries the IPv4 network address if the peer's remote-address is an IPv6 address.

The no form of the command resets network-address configured for the peer.

Syntax **neighbor < ip-address > network-address <random_str>**

no neighbor < ip-address > network-address <random_str>

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<random_str>` - Configures the Remote IP address of the peer.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Notes:

- This command executes only if Peer/ Peer Groupis created and Peer AS is configured.
- The peer's remote network address can be configured only after configuring the peer's remote address and the corresponding local interface.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 gateway 10.0.0.1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `show ip bgp` – Displays the BGP related information.
- `address-family` - Enters the router into the address-family router configuration mode.

neighbor – default-originate

Command Objective This command enables advertisement of the default route to the peer or neighbor for use as a default route. This command overrides the global default route configuration and sends a default route to the peer with self next-hop.

The advertisement occurs irrespective of the presence of default route in FDB.This command does not require the presence of 0.0.0.0 in the local router. When used with a route map, the default route 0.0.0.0 is injected if the route map contains a match ip address clause. The route map can contain other match clauses also.

The no form of the command disables advertisement of the default route to the peer.

Syntax **neighbor <ip-address|peer-group-name> default-originate**

no neighbor <ip-address|peer-group-name> default-originate

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<peer-group-name>` - Configures a BGP peer group by using the peer- group-name argument. The members of the peer group will inherit the characteristic configured with this command.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default The advertisement of default route to the peer is disabled.

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 default-originate
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `show ip bgp info` - Displays the general information about BGP protocol.
- `address-family` - Enters the router into the address-family router configuration mode.

neighbor – send-community

Command Objective This command sends community attribute to a BGP neighbor and enables advertisement of community attributes (standard/extended) to peer.

The no form of the command disables advertisement of community attributes (standard/extended) to peer.

Syntax **neighbor < ip-address|peer-group-name > send-community {both | standard | extended}**

no neighbor < ip-address|peer-group-name > send-community {both | standard |extended}

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<peer-group-name>` - Configures a BGP peer group by using the peer- group-name argument. The

members of the peer group will inherit the characteristic configured with this command.

- `send-community` - Sends the Communities to peer.
    - both - Sends both standard and extended communities to peer.
    - standard - Sends only standard communities to the peer.
    - extended - Sends only extended communities to the peer.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default send-community - both

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 send-community both
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `show ip bgp info` - Displays the general information about BGP protocol.
- `address-family` - Enters the router into the address-family router configuration mode.

neighbor – capability

Command Objective This command enables the specific BGP capability to be advertised and received from the peer.

The no form of the command disables the capability for the peer.

Syntax **neighbor <ip-address|peer-group-name> capability{ipv4-unicast|ipv6-unicast|route-refresh | orf prefix-list {send | receive | both}}**

no neighbor <ip-address|peer-group-name> capability {ipv4-unncast|ipv6-unicast|route-refresh | orf prefix-list {send | receive | both}}

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<peer-group-name>` - Configures a BGP peer group by using the peer- group-name argument. The members of the peer group will inherit the characteristic configured with this command.
- `ipv4-unicast` - Sets the IPv4 unicast address family capability.
- `ipv6-unicast` - Sets the MP IPv6 unicast address family capability.
- `route-refresh` - Sets the Route refresh capability.
- `orf prefix-list` - Enables address prefix-based Outbound Route Filter (ORF) for the specified BGP peer group.
    - `send` - Enables ORF send capability.

- `receive` - Enables ORF recieve capability.
- `both` - Enables both send and receive ORF Capability.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default By default ipv4-unicast and route-refresh capabilities are enabled for a peer

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 capability ipv4-unicast
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.

bgp nonbgproute-advt

Command Objective This command configures the peer type to whom non-bgp routes can be propagated and controls the advertisement of Non-BGP routes either to the external peer or both to internal and external peer.

The no form of the command resets the Non BGP routes advertisement policy to its default value. The Administrator can effectively control the advertisement of the route learnt through Redistribution.

Syntax **bgp nonbgproute-advt <external|both>**

no bgp nonbgproute-advt

Parameter Description

- `external` - Indicates that the non-BGP routes can be exported only to to external peers. All types of non-bgp routes can be propagated to external peers.
- `both` - Indicates that the non-BGP routes can be propagated to both internal and external peers.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default both

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# bgp nonbgproute-advt both
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp info` – Displays the general information about BGP protocol.

redistribute

Command Objective This command controls redistribution of Direct, Static, IGP(OSPF,RIP) routes into BGP and configures the protocol from which the routes have to be redistributed into BGP after applying the specified route map. If this is set to enable, only the routes from the protocols are imported into BGP and BGP routes will not be distributed to IGP. If this is set as disable, then the routes learned from protocols are removed from BGP and no route is either distributed to or imported from IGP.

The no form of the command disables the redistribution of routes from the given protocol into BGP. The route map is disassociated from the redistribution, if the no form of the command specifies the route map.

Syntax **redistribute <static|connected|rip|ospf|all> [route-map <string(20)>] [metric <integer>]**

no redistribute <static|connected|rip|ospf|all> [route-map <string(20)>] [metric]

Parameter Description

- `static` - Redistributes routes, configured statically, in the BGP routing process.
- `connected` - Redistributes directly connected networks routes, in the BGP routing process.
- `rip` - Redistributes routes that are learnt by the RIP process, in the BGP routing process.
- `ospf` - Redistributes routes, that are learnt by the OSPF process, in the BGP routing process.
- `all` - Redistributes routes, that are learnt by the all processes (RIP,OSPF, statically configured and connected routes), in the BGP routing process
- `route-map <string(20)>` - Identifies the specified route-map in the list of route-maps during redistribution of routes to BGP. If this is not specified, all routes are redistributed. This value is a string with the maximum size as 20.
- `metric <integer>` - Specifies the metric value for the routes to redistribute to bgp. This value ranges between 0 and 4294967295. If the metric value not specified, default metric value is considered.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Redistribution is disabled

Note: Redistribution can be configured for only one route map. Another route map can be assigned, only if the already assigned route map is disabled.

Example

```
Your Product(config-router)# redistribute all route-map rm metric 500
```

Related Command(s) `router bgp` – Sets the AS number of the BGP Speaker.

import route

Command Objective This command adds non-BGP IP routes imported into the BGP RIB and allows importing a static route into BGP, after updating the RIB tree, if there is any change in the best route selected, then the route is updated to the Common Forwarding table.

Syntax **import route ip-address prefixlen nexthop metric ifindex protocol action route-count**

Parameter Description

- `ip-address` - Configures the Prefix of the route to be imported.
- `prefixlen` - Configures the number of high-order bits in the IP address These bits are common among all hosts within a network. This value ranges between 1 and 32.
- `nexthop` - Configures the Nexthop IP address for the route.
- `metric` - Configures the metric value for the routes being imported. This value ranges between 1 and 2147483647.
- `ifindex` - Configures the interface index of the route. This value ranges between 1 and 2147483647.
- `protocol` - Configures the Protocol value for the non-BGP routes. The values can be:
  - 2 **–** Local.
  - 3 **–** Static.
  - 8 **–** RIP.
  - 13 **–** OSPF

  Note: Only STATIC routes (protocol 3) can be added through Common Forwarding table. All non-BGP protocol (Local, Static, RIP, OSPF) routes can be viewed.
- `action` - Controls addition or deletion of the non bgp routes. The options are:
  - Add **–** Specifies the addition of non bgp routes.
  - Delete- Specifies the deletion of non bgp routes.
- `route-count` - Configures the number of routes to be imported.

Mode BGP Router Configuration Mode

Example

```
Your Product(config-router)# import route 23.45.0.1 10 23.45.0.10 10 2 3
add 4
```

Related Command(s) `router bgp` – Sets the AS number of the BGP Speaker.

bgp always-compare-med

Command Objective This command enables the comparison of Multi Exit Discriminator (MED) for routes received from different 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.

The no form of the command disables the comparison of MED for routes received from different autonomous system. MED will be compared only for routes from same neighbor autonomous system.

Syntax **bgp always-compare-med**

no bgp always-compare-med

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default The comparison of MED for routes received from different autonomous system is disabled

Example

```
Your Product(config-router)# bgp always-compare-med
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp info` - Displays the general information about BGP protocol.
- `address-family` - Enters the router into the address-family router configuration mode.

default-metric

Command Objective This command configures the default IGP metric value for routes redistributed into BGP with the redistribute command. A default metric can be configured to solve the problem of redistributing routes with incompatible metrics. Assigning the default metric will allow redistribution to occur. This value ranges between 0 and 2147483647.

The no form of the command resets the Default IGP Metric value to its default value 0. If configured to 0, the metric received from the IGP route will be used. If configured to any other value, the MED value of the redistributed routes take this value. This value has no effect on the Direct routes.

Syntax **default-metric <Default Metric Value(0-2147483647)>**

no default-metric

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 0

Example

```
Your Product(config-router)# default-metric 300
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp info` - Displays the general information about BGP protocol.
- `address-family` - Enters the router into the address-family router configuration mode.

bgp med

Command Objective This command configures an entry in BGP4 MED Table and contains the MED values that are to be assigned to routes.

The no form of the command deletes the entry from MED Table,.BGP4 MED table. The entry will not be matched when the MED value for an update is calculated, if the prefix length is set as zero.

Syntax **bgp med <1-100> remote-as <AS no> <ip-address> <prefixlen> [intermediate-as <AS-no list- AS1,AS2,...>] value <value> direction {in|out}[override]**

no bgp med <1-100>

Parameter Description

- `med <1-100>` - Configures the entry containing information about the MED value. This value ranges between 1 and 100.
- `remote-as < AS no >`- Configures the Autonomous system number that identifies the BGP router to other routers and tags the routing information passed along. This value ranges between 0 and 4294967295 or 0.1 to 65535.65535.

  Notes:

  - When four-byte-asn is enabled, this value ranges between 0 and 4294967295or between 0.0 and 65535.65535
  - When four-byte-asn is disabled, this value ranges between 0 and 65535. or between 0.0 and 0.65535
  - When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.0 to 65535.65535
  - A value of zero indicates that this entry is not valid and will not be matched for when the MED value for an update is calculated
- `<ip-address>`- Configures the Route-prefix on which MED policy needs to be applied.
- `<prefixlen>` - Configures the number of high-order bits in the IP address. This is the length of the IP address prefix in the Network Layer Reachability Information (NLRI) field . These bits are common among all hosts within a network. This value ranges between 0 and 32.

  Note: A value of zero indicates that this entry is not valid and will not be matched for when the MED value for an update is calculated.

- `intermediate-as<AS-no list- AS1,AS2,...>` - Configures the sequence of intermediate Autonomous system numbers through which the route update is expected to travel. This is a Comma separated list of AS numbers that are to be checked against the AS_PATH attribute of the updates. This valus is a string with the maximum size as 100.
- `Value <value>` - Configures the value assigned to the MED attribute for the route present in NLRI. This value ranges between 0 .and 2147483647.
- `direction` - Configures the direction of application of MED policy.
  - `in` – Indicates that on received route-update with other matching attributes like as-number, intermediate-as numbers

  - `out` - Indicates that on route-update that needs to be advertised to peer
- `override` - Decides whether the configured MED value will override the received MED value.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode **Default**

- remote-as - 0
- Prefixlen - 0
- direction - In
- Value - 0

Example

```
Your Product(config-router)# bgp med 5 remote-as 200 212.23.45.0 24
intermediate-as 150 value 50 direction in override
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp med` – Displays the contents of MED table
- `address-family` - Enters the router into the address-family router configuration mode.
- `ip bgp four-byte-asn` - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system
- `bgp asnotation dot` - Changes the output format of BGP ASNs from asplain to asdot notation.

bgp local-preference

Command Objective This command configures an entry in the Local Preference Table. This table contains the value that is to be assigned to the Local Preference attibute.

The no form of the command deletes the entry from Local Preference Table.

Syntax **bgp local-preference <1-100> remote-as <AS no> <ip-address> <prefixlen> [intermediate-as <AS-no list-AS1,AS2,...>] value <value> direction {in|out} [override]**

no bgp local-preference <1-100>

Parameter Description

- `local-preference <1-100>` - Configures the local preference index. This value ranges between 1 and 100.
- `remote-as < AS no >` - Configures the Autonomous system number that identifies the BGP router to other routers and tags the routing information passed along. This value ranges between 0 and 4294967295 or 0.1 to 65535.65535.

  Notes:

  - When four-byte-asn is enabled, this value ranges between 0 and 4294967295or between 0.0 and 65535.65535
  - When four-byte-asn is disabled, this value ranges between 0 and 65535. or between 0.0 and

    0.65535
    - When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.0 to 65535.65535
- `<ip-address>` - Configures the route prefix in the Network Layer Reachability Information on which local-preference policy needs to be applied. The input route ip address can be an ipv4 or an ipv6 address.
- `<prefixlen>` - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges between 0 and 32 for ipv4 address and 0 to 128 for ipv6 address.

  Notes: A value of zero indicates that this entry is not valid and will not be matched for when the MED value for an update is calculated.

- `intermediate-as<AS-no list- AS1,AS2,...>` - Configures the sequence of intermediate AS numbers through which the route update is expected to travel or a Comma separated list of AS numbers that are to be checked against the AS_PATH attribute of the updates. This value is a list with the maximum size as 100.
- `Value <value>` - Configures the local-preference value that needs to be associated with the route-update. This value ranges between 0 .and 2147483647.
- `direction` - Specifiies the direction of the application of local-preference policy with which the entry is to be associated
    - `in` – Indicates that on received route-update with other matching attributes like as-number, intermediate-as numbers
    - `out` - Indicates that on route-update that needs to be advertised to peer
- `override` - Decides whether configured local-preference value overrides the received local-preference value. If this keyword is not specified, then the received value will have precedence over configured value.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default

- remote-as - 0
- direction - In
- Value - 100
- ip-address – 0.0.0.0
- Prefixlen - 0

Example

```
Your Product(config-router)# bgp local-preference 5 remote-as 200 21.3.0.0
16 intermediate-as 150 value 250 direction out override
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp local-pref` – Displays the contents of local preference table.
- `address-family` - Enters the router into the address-family router configuration mode.
- `ip bgp four-byte-asn` - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system
- `bgp asnotation dot` - Changes the output format of BGP ASNs from asplain to asdot notation.

bgp update-filter

Command Objective This command configures an entry in Update Filter Table which contains rules to filter out updates based on the AS from which it is received, Network Layer Reachability Information (NLRI) and AS through which it had passed.

The no form of the command deletes the entry from Update Filter Table.

Syntax **bgp update-filter <1-100> {permit|deny} remote-as <AS no> <ip-address> <prefixlen> [intermediate-as <AS-no list-AS1,AS2,...>] direction {in|out}**

no bgp update-filter <1-100>

Parameter Description

- `update-filter <1-100>` - Configures the entry containing information about the updates that are to be filtered. This value ranges between 1 and 100.
- `permit` - Allows the route to pass filter policy test.
- `deny` - Filters the routes when it passes through filter policy test
- `remote-as < AS no >`- Configures the Autonomous system number that identifies the BGP router to other routers and tags the routing information passed along. This value ranges between 0 and 4294967295 or 0.1 to 65535.65535.

  Notes:

  - When four-byte-asn is enabled, this value ranges between 0 and 4294967295or between 0.0 and 65535.65535
  - When four-byte-asn is disabled, this value ranges between 0 and 65535. or between 0.0 and 0.65535
  - When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.0 to 65535.65535
- `<ip-address>` - Configures the route prefix in the Network Layer Reachability Information on which the filter needs to be applied.
- `<prefixlen>` - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges between 0 and 32 for ipv4 address and 0 to 128 for ipv6 address.

  Note: The NLRI field will not be matched if the prefix length is set as zero.

- `intermediate-as<AS-no list- AS1,AS2,...>` - Configures the sequence of intermediate AS numbers through which the route update is expected to travel or a Comma separated list of AS numbers that are to be checked against the AS_PATH attribute of the updates. This value is a list with the maximum size as 100.
- `direction` - Specifiies the direction of the application of filters with which the entry is to be associated
  - `in` **–** Indicates that on received route-update with other matching attributes like as-number, intermediate-as numbers
  - `out` - Indicates that on route-update that needs to be advertised to peer

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default

- remote-as - 0
- direction - In
- ip-address – 0.0.0.0
- Prefixlen - 0

Example

```
Your Product(config-router)# bgp update-filter 6 deny remote-as 145
72.93.0.0 14 intermediate-as 150 direction in
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp filters` – Displays the contents of filter table
- `address-family` - Enters the router into the address-family router configuration mode.
- `ip bgp four-byte-asn` - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system
- `bgp asnotation dot` - Changes the output format of BGP ASNs from asplain to asdot notation.

aggregate-address index

Command Objective This command creates an aggregate entry in a BGP or multiprotocol BGP routing table if any more-specific BGP or multiprotocol BGP routes are available that fall in the specified range. The entries in the table specifies the IP address based on which the routing information has to be aggregated. The aggregate route will be advertised as coming from autonomous system. The atomic aggregate attribute will be set only if some of the information in the AS PATH is missing in the aggregated route, else it will not be set.

The no form of the command deletes the specified entry from the aggregate table.

Syntax **aggregate-address index <1-100> <ip-address> <prefixlen> [summary-only] [as-set] [suppress-map map-name] [advertise-map map-name] [attribute-map map-name**

no aggregate-address index <1-100>

Parameter Description

- `index <1-100>` - Configures the entry containing information about the IP address on which the aggregation has to be done. This value ranges between 1 and 100.
- `<ip-address>` - Configures route prefix in the Network Layer Reachability Information on which aggregate policy needs to be applied
- `<prefixlen>` - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges between 0 and 32 for IPv4 address and between 0 and 128 for IPv6 Address.
- `summary-only` - Specifies that aggregated (summarized) route alone will be sent to the peers.

  Note: If this is not specified , both the summary and the more-specific routes based on which the summary entry was generated are be advertised to the peers.

- `as-set` - Generates autonomous system set path information.
- `suppress-map map-name` - Specifies the name of the route map used to select the routes to be suppressed. The route map contains the rules for suppressing the more-specific routes in forming the aggregate route.. When suppress-map configuration is used along with summaryonly option, summary-only configuration command does'nt have any effect. And the more-specific routes that the suppress-map suppresses are not advertised. Other routes are advertised in addition to the aggregated route. This value is a string with a maximum length of 20.
- `advertise-map map-name` - Specifies the name of the route map used to select for forming aggregate routes. The route map contains the rules for selecting specific routes for aggregation Other routes are advertised. When advertise-map is used, only advertise-map influences the creation of aggregate entry. In absence of advertise-map, the aggregate route inherits the attributes of the more specific routes, both suppressed and unsuppressed.This value is a string with a maximum length of 20.
- `attribute-map map-name` - Specifies the name of the route map used to form the attribute of the aggregate route. The route map contains the rules for setting the attributes for the aggregated route. When attribute-map and advertise-map along with autonomous system set path information are enabled and other configurations, the attribute-map overrides the attribute that is formed with the routes selected by the advertise-map.. This value is a string with a maximum length of 20.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Note: The IP address and the prefix length can be configured, only if the Aggregate admin status of the BGP is down.

Example

```
Your Product(config-router)# aggregate-address index 1 21.1.0.0 16 summary-only
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.

- `show ip bgp aggregate` – Displays the contents of aggregate table
- `address-family` - Enters the router into the address-family router configuration mode.

bgp cluster-id

Command Objective This command configures the Cluster ID for the Router Reflector of the BGP cluster which has more than one route reflector. This value ranges between 1 and 4294967295.

Usually in a cluster of clients with single route reflector the cluster is identified by the router ID of the route reflector. In order to increase redundancy and avoid a single point of failure, a cluster might have more than one route reflector. In this case, all route reflectors in the cluster must be configured with the 4-byte cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster.

The no form of the command resets the Cluster ID for the Route Reflector.

Syntax **bgp cluster-id {cluster id value ip_address/integer}**

no bgp cluster-id

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Example
```
Your Product(config-router)# bgp cluster-id 10.0.0.1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp rfl info` – Displays information about RFL feature.
- `address-family` - Enters the router into the address-family router configuration mode.

client-to-client reflection

Command Objective This command configures the Route Reflector to support route reflection to Client Peers. By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. If the clients are fully meshed, route reflection is not required.

The no form of the command disables client-to-client reflection. If disabled, then Route Reflector will not advertise routes learnt from a client peer to other client peers. This occurs when all peers within a cluster are fully-meshed and the client peer itself is able to advertise routes to other clients of the route-reflector.

Syntax **bgp client-to-client reflection**

no bgp client-to-client reflection

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Route Reflector will reflect routes learnt from a client peer to all other client peers.

Example

```
Your Product(config-router)# bgp client-to-client reflection
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp rfl info` – Displays information about RFL feature.
- `address-family` - Enters the router into the address-family router configuration mode.

neighbor - route-reflector-client

Command Objective This command controls client-to-client reflection and configures the specified Peer as Client of the Route Reflector. All the neighbors configured with this command will be members of the client group and the remaining IBGP peers will be members of the nonclient group for the local route reflector.

The no form of the command resets the Peer as conventional BGP Peer.

Syntax **neighbor <ip-address | peer-group-name> route-reflector-client**

no neighbor <ip-address | peer-group-name> route-reflector-client

Parameter Description

- `<ip-address>` - Configures the Peer's Remote IP address of the BGP neighbor being identified as a client.
- `<peer-group-name>` - Configures a BGP peer group by using the peer- group-name argument. Tthe members of the peer group will inherit the characteristic configured with this command.

Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode BGP Router Configuration Mode/ Address Family Router Configuration Mode

Note: This command executes only if Peer is created.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 route-reflector-client
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor` - remote-as – Creates a Peer and initiates the connection to the peer
- `address-family` - Enters the router into the address-family router configuration mode
- `show ip bgp rfl info` – Displays information about RFL feature

bgp comm-route

Command Objective This command configures an entry in additive or delete community table for a given destination.

The no form of the command removes the entry from additive or delete community table.

Syntax **bgp comm-route {additive|delete} <ip-address> <prefixlen> comm-value <4294967041-4294967043,65536-4294901759>**

no bgp comm-route {additive|delete} <ip-address> <prefixlen> comm-value <4294967041-4294967043,65536-4294901759>

Parameter Description

- additive - Adds associated community value with the already existing communities in the route update.
- delete - Removes the community attribute from the route-prefix when it passes through the filter process.
- <ip-address> - Configures the Route prefix on which community policy needs to be applied.
- <prefixlen> - Configures the IP prefix length for the destination. These bits are common among all hosts within a network. This value ranges between 1 and 32.
- comm-value <4294967041-4294967043,65536-4294901759> - Configures the Community attribute value. This value ranges between 4294967041 and 4294967043 or between 65536 and 4294901759.

Mode BGP Router Configuration Mode/ Address Family Router Configuration Mode

Note: This command executes only if Peer is created.

Example

```
Your Product(config-router)# bgp comm-route additive 24.5.0.0 16 comm-value
429490
```

Related Command(s)

- router bgp – Sets the AS number of the BGP Speaker.
- address-family - Enters the router into the address-family router configuration mode
- show ip bgp community– Displays the contents of route/peer/filter/policy community tables.

bgp comm-filter

Command Objective This command allows/ filters the community attribute while receiving or advertising. The rules to filter out the updates are based on the AS from which it is received, NLRI and AS through which it had passed.

The no form of the command removes the filter policy for the community attribute.

Syntax **bgp comm-filter <comm-value(4294967041-4294967043,65536-4294901759)> <permit|deny> <in|out>**

no bgp comm-filter <comm-value(4294967041-4294967043,65536-4294901759)> <permit|deny> <in|out>

Parameter Description

- `comm-value(4294967041-4294967043,65536-4294901759)>` - Configures the Community Attribute Value. This value ranges between 4294967041 and 4294967043 or between 65536 and 4294901759.
- `permit` - Allows a particular community attribute to be received or advertised in updates.
- `deny` - Filters the routes containing the community attribute value in received or advertised updates.
- `in` - Configures the direction of route-updates on which the community filter policy needs to be applied as in. This indicates that the community filter needs to be applied on received routes.
- `out` - Configures the direction of route-updates on which the community filter policy needs to be applied as out. This indicates that the community filter needs to be applied on routes advertised to peers.

Mode BGP Router Configuration Mode/ Address Family Router Configuration Mode

Default permit

Example

```
Your Product(config-router)# bgp comm-filter 75100 deny in
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode
- `show ip bgp community`– Displays the contents of route/peer/filter/policy community tables.

bgp comm-policy

Command Objective This command configures the community attribute advertisement policy for specific destination.

The no form of the command removes the community attribute advertisement policy for specific destination.

Syntax **bgp comm-policy <ip-address> <prefixlen> <set-add|set-none|modify>**

no bgp comm-policy <ip-address> <prefixlen>

Parameter Description

- `<ip-address>` - Configures the Route prefix on which community policy needs to be applied.
- `<prefixlen>` - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges between 1 and 32.
- `set-add` - Sends only the configured additive communities with associated route.
- `set-none` - Sends the associated route without any communities.

- `modify` - Removes the associated route with received delete communities and adds the configured additive communities.

Mode BGP Router Configuration Mode/ Address Family Router Configuration Mode

Default modify

Example

```
Your Product(config-router)# bgp comm-policy 24.5.0.0 10 set-none
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode
- `show ip bgp community`– Displays the contents of route/peer/filter/policy community tables.

bgp ecomm-route

Command Objective This command configures an entry in additive or delete extended community table.

The no form of the command removes the entry from additive or delete extended community table.

Syntax **bgp ecomm-route {additive|delete} <ip-address> <prefixlen> ecomm-value <value(xx:xx:xx:xx:xx:xx:xx:xx)>**
no bgp ecomm-route {additive|delete} <ip-address> <prefixlen> ecomm-value <value(xx:xx:xx:xx:xx:xx:xx:xx)>

Parameter Description

- `additive` - Adds associated extended-community value with the already existing communities in the route update.
- `delete` - Removes the extended-community attribute from the route-prefix when it passes through the filter process.
- `<ip-address>` - Configures the Route prefix on which community policy needs to be applied.
- `<prefixlen>` - Configures the IP prefix length for the destination. These bits are common among all hosts within a network. This value ranges between 1 and 32.
- `ecomm-value <value(xx:xx:xx:xx:xx:xx:xx:xx)>` - Configures the Extended Community Attribute Value. This is an octet string value.

Mode BGP Router Configuration Mode/ Address Family Router Configuration Mode

Example

```
Your Product(config-router)# bgp ecomm-route additive 12.0.0.0 2 ecomm-
value 01:01:22:33:44:55:66:77
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.

- `address-family` - Enters the router into the address-family router configuration mode
- `show ip bgp extcommunity` – Displays the contents of route ext-community route tables.

bgp ecomm-filter

Command Objective This command allows/ filters the extended community attribute while receiving or advertising.

The no form of the command removes the filter policy for the extended community attribute.

Syntax **bgp ecomm-filter <ecomm-value(xx:xx:xx:xx:xx:xx:xx:xx)> {permit|deny} {in|out}**

no bgp ecomm-filter <ecomm-value(xx:xx:xx:xx:xx:xx:xx:xx)> {permit|deny} {in|out}

Parameter Description

- `<ecomm-value(xx:xx:xx:xx:xx:xx:xx:xx)>` - Configures the extended community value. This is an octet string value in the form xx:xx:xx:xx:xx:xx:xx:xx.
- `permit` - Allows the route -update with the associated extended community value to pass the filter test.
- `deny` - Denies the route-update with the associated extended community value to pass the filter test.
- `in` - Configures the incoming direction of applied filter.
- `out` - Configures the outgoing direction of applied filter.

Mode BGP Router Configuration Mode/ Address Family Router Configuration Mode

Default permit

Example

```
Your Product(config-router)# bgp ecomm-filter 01:01:22:33:23:43:44:22 deny
in
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode
- `show ip bgp extcommunity` – Displays the contents of ext-community route table.

bgp ecomm-policy

Command Objective This command configures the extended community attribute advertisement policy for specific destination.

The no form of the command removes the extended community attribute advertisement policy for specific destination.

Syntax **bgp ecomm-policy <ip-address> <prefixlen > <set-add|set-none|modify>**

no bgp ecomm-policy <ip-address> <prefixlen>

Parameter Description

- `<ip-address>` - Configures the route prefix on which extended community policy needs to be applied.
- `<prefixlen>` - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges between 1 and 32.
- `set-add` - Sends associated route with configured additive extended-communities only.
- `set-none` - Sends the associated route without any extended-communities.
- `modify` - Strips the associated route with received delete extended communities and adds the configured additive extended communities.

Mode BGP Router Configuration Mode/ Address Family Router Configuration Mode

Default modify

Example

```
Your Product(config-router)# bgp ecomm-policy 12.0.0.0 14 set-add
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode
- `show ip bgp extcommunity` – Displays the contents of policy ext-community route tables.

bgp confederation identifier

Command Objective This command configures the BGP confederation identifier which specifies the confederation to which the autonomous systems belong to. This value ranges between 1 and 4294967295 or 0.1 to 65535.65535.

The no form of the command removes the configured BGP confederation identifier and resets the identifier to its default value.

Notes:

- If this value is already configured to a non-zero value, it must be reset to zero (using no form of the command) before reconfiguring.
- When four-byte-asn is enabled, this value ranges between 1 and 4294967295or between 0.1 and 65535.65535.
- When four-byte-asn is disabled, this value ranges between 1 and 65535. or between 0.1 and 0.65535.
- When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.65535.

Syntax **bgp confederation identifier <AS no>**

bgp confederation identifier <AS no>

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 0

Example

```
Your Product(config-router)# bgp confederation identifier 1000
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp confed info` – Displays information about confederation feature.
- `address-family` - Enters the router into the address-family router configuration mode.
- `ip bgp four-byte-asn` - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system.
- `bgp asnotation dot` - Changes the output format of BGP ASNs from asplain to asdot notation.

bgp confederation peers

Command Objective This command configures the Autonomous Systems that belongs to the confederation. The autonomous systems specified in this command are visible internally to a confederation. Each autonomous system is fully meshed within itself. This value ranges between 1 and 4294967295 or 0.1 to 65535.65535.

Notes:

- When four-byte-asn is enabled, this value ranges between 1 and 4294967295or between 0.1 and 65535.65535.
- When four-byte-asn is disabled, this value ranges between 1 and 65535. or between 0.1 and 0.65535.
- When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.65535.

The no form of the command removes the Autonomous Systems from the confederation.

Syntax **bgp confederation peers <AS no>**

no bgp confederation peers <AS no>

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default By default no AS will be added to the confederation

Note: This command executes only if the Peer AS number is not equal to BGP Speaker Local AS number.

Example

```
Your Product(config-router)# bgp confederation peers 100
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp confed info` – Displays information about confederation feature.
- `ip bgp four-byte-asn` - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system.
- `bgp asnotation dot` - Changes the output format of BGP ASNs from asplain to asdot notation.

bgp bestpath med confed

Command Objective This command enables MED comparison among paths learnt from confederation peers. The comparison between MEDs is only made if there are no external autonomous systems in the path. If there is an external autonomous system in the path, then the external MED is passed transparently through the confederation, and the comparison is not made.

The no form of the command disables MED comparison among paths learnt from confed peers and prevent the software from considering the MED attribute in comparing paths.

Syntax **bgp bestpath med confed**

no bgp bestpath med confed

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default In BGP route selection algorithm, MED attributes comparison between two routes originated within the local confederation is disabled.

Example

```
Your Product(config-router)# bgp bestpath med confed
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp confed info` – Displays information about confederation feature.
- `address-family` - Enters the router into the address-family router configuration mode.

neighbor - password

Command Objective This command enables Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers where each segment sent on the TCP connection between the peers is verified. The MD5 authentication must be configured with the same password on both BGP peers; else, the connection between them will not be made.

The no form of the command resets the TCP-MD5 password set for the peer.

Syntax **neighbor <ip-address> password password-string**

no neighbor <ip-address> password

Parameter Description

- `<ip-address>` - Specifies the IP address of the BGP peer for which the TCP MD5 Authentication password is to be set.
- `password- string` - Configures the TCP MD5 Authentication Password that has to be sent with all TCP packets originated from the peer. This value is a string with the maximum size as 80.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default By default , the MD5 password setting is disabled.

Note: This command executes only if Peer is created

Example

```
Your Product(config-router)# neighbor 10.0.0.2 password abcdef
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor` - remote-as – Creates a Peer and initiates the connection to the peer.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp info` – Displays the general information about BGP protocol.

address-family

Command Objective This command enters the router into the address-family router configuration mode. Routing information is advertised for IPv4 address family when a BGP session is configured, unless the default advertising is reset.

The no form of the command deletes the peers belonging to the IPV4, IPv6 and VPNv4 address family.

Syntax **address-family [ipv4 | ipv6] [vrf <vrf-name>]**

no address-family { ipv4 | ipv6} [vrf <vrf-name>]

Parameter Description

- `ipv4` - Configures session that carries standard IPv4 address prefixes.
- `ipv6` - Configures session that carries standard IPv6 address prefixes.
- `rip` - Redistributes routes that are learnt by the RIP process, in the BGP routing process.
- `vrf <vrf-name>` - Configures the address-family router configuration for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode BGP Router Configuration Mode

Example

```
Your Product(config-router)# address-family ipv4
Your Product(config-router-af4)#
Your Product(config-router)# address-family ipv6
Your Product(config-router-af6)#
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp` – Displays the BGP related information.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - interval` – Configures neighbor interval.
- `neighbor - timers`– Configures neighbor KeepAlive Time and Hold Time Intervals.
- `neighbor - shutdown` – Disables the Peer session.
- `neighbor - update-source` - Configures the source-address for routing updates and for TCP connection establishment with a peer.
- `neighbor - gateway` - Configures gateway router's address that will be used as nexthop in the routes advertised to the peer.
- `neighbor - activate` – Enables default capabilities for the peer and restarts the connnection to the peer if capabilities negotiated change.
- `neighbor - delay open` - Configures a delay in sending the first OPEN message to the BGP peer for a specific time period.
- `neighbor - maximum prefix` - Configures the maximum number of peers supported by BGP.
- `neighbor - damp-peer-oscillations` - Enables the damp peer oscillation option.
- `neighbor - allow-autostop` - Enables the auto stop option to stop the BGP peer and BGP connection automatically.
- `neighbor - connect-retrycount` - Sets the retry count for the BGP peer.
- `neighbor - transport connection-mode` - Configures the BGP Peer Transport Connection status as active or passive.
- `neighbor - peer-group` – Creates a peer group.
- `tcp-ao mkt key-id - receive-key-id` - Creates a TCP-AO MKT in the BGP instance.
- `neighbor -tcp-ao` - sets BGP peer TCP-AO configurations.
- `neighbor - tcp-ao mkt` - Associates a TCP-AO MKT to the BGP peer.

bgp graceful-restart

Command Objective This command enables graceful restart capability in router which allows forwarding of data packets to continue along known routes, while the routing protocol information is being restored following a processor switch over. When graceful restart is enabled, peer networking devices are informed, through protocol extensions prior to the event.

The no form of the command disables the graceful restart capability and resets the restart-time or stalepath-time to the default value.

Syntax **bgp graceful-restart [restart-time <(1-4096)<seconds>] [stalepath-time <(90-3600)<seconds>]**

no bgp graceful-restart [restart-time] [stalepath-time]

Parameter Description

- `restart-time<(1-4096)<seconds>` - Configures the estimated time (in seconds) taken for re-establishing a BGP session after restart. The default value for this should be less than or equal to Hold Time carried in open message. This value ranges between 1 and 4096 seconds.
- `stalepath-time<(90-3600)<seconds>` - Configures the Time (in seconds) until which the router retains the stale routes. This value ranges between 90 and 3600 seconds.

Mode BGP Router Configuration Mode

Default

- Graceful Restart is disabled.
- restart-time -90 seconds.
- stalepath-time-150 seconds.
- If those time are default value, it will not display bgp graceful-restart command in the running config.
- When creating/deleting a BGP group, the graceful restart will be enable/disable.

Example

```
Your Product(config-router)# bgp graceful-restart restart-time 33 stalepath
789
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp timers` - Displays the value of BGP timers.
- `show ip bgp info` – Displays the general information about BGP protocol.

bgp update-delay

Command Objective This command configures the selection deferral time interval. This time interval represents the time (in seconds) until which the router defers its route selection. This value ranges between 60 and 1800 seconds.

This time interval should be configured to provide enough time for all the peers of the restarting speaker to send all the routes to the restarting speaker.

The no form of the command resets the time interval to its default value.

Syntax **bgp update-delay <(60-1800)seconds>**

no bgp update-delay

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 60 seconds

Example `Your Product(config-router)# bgp update-delay 90`

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp timers` - Displays the value of BGP timers.
- `address-family` - Enters the router into the address-family router configuration mode.

restart-support

Command Objective This command enables the graceful restart support. Graceful restart support is provided for both planned and unplanned restart, if the command is executed without any option.

The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent.

The no form of the command disables the graceful restart support.

Syntax **restart-support [plannedOnly]**

no restart-support

Parameter Description `plannedOnly` - Supports only the planned restarts (such as restarting a control plane after a planned downtime).

Mode BGP Router Configuration Mode

Default Graceful restart support is disabled.

Note: This command executes only if the graceful restart capability is disabled.

Example `Your Product(config-router)# restart-support`

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `no bgp graceful-restart` - Disables the graceful restart capability and resets the restart-time or stalepath-time to default value.
- `show ip bgp restartsupport` - Displays the restart support of the BGP.

restart-reason

Command Objective This command configures the reason for the graceful restart of the BGP router. The reason for restart can be unknown, software upgrade, scheduled restart or switch to redundant router.

The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent.

The no form of the command resets the reason for restart.

Syntax **restart-reason [{unknown|softwareRestart|swReloadUpgrade}]**

no restart-reason [{unknown|softwareRestart|swReloadUpgrade}]

Parameter Description

- `unknown` - Configures reason for graceful restart of the BGP router as restart due to unplanned events (such as restarting after a crash).
- `softwareRestart` - Configures reason for graceful restart of the BGP router as restart due to restart of software.
- `swReloadUpgrade` - Configures reason for graceful restart of the BGP router as restart due to reload or upgrade of software.

Mode BGP Router Configuration Mode

Default softwareRestart

Example

```
Your Product(config-router)# restart-reason swReloadUpgrade
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp restartreason` - Displays the restart reason of the BGP.

distribute-list route-map

Command Objective This command enables route map filtering for inbound or outbound routes and defines the conditions for distributing the routes from one routing protocol to another.

The no form of the command disables inbound filtering for the routes.

Syntax **distribute-list route-map <name(1-20)> {in | out}**

no distribute-list route-map <name(1-20)> {in | out}

Note: This command executes only if Peer is created.

Parameter Description

- `<name(1-20>` - Specifies the name of the Route Map to be used for filtering. This value is a string with the maximum size as 20.
- `in` - Sets filtering for inbound routes.
- `out` - Sets filtering for outbound routes.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default By default , the MD5 password setting is disabled.

Note: Only one route map can be set for inbound or outbound routes. Another route map can be assigned, only if the already assigned route map is disabled.

Example

```
Your Product(config-router)# distribute-list route-map rmap-test in
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode.

distance

Command Objective This command enables the administrative distance value which is used as a preference parameter in IP for best route selection (. This value ranges between 1 and 255.

The no form of the command disables the administrative distance.

Syntax **distance <1-255> [route-map <name(1-20)>]**

no distance [route-map <name(1-20)>]

If Routemap is disabled

distance <1-255>

no distance

Parameter Description

- `route-map <name(1-20)>` - Configures the name of the Route Map for which the distance value should be enabled and set. This value is a string with the maximum size as 20.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Note: Distance can be set for only one route map. Another route map can be assigned, only if the already assigned route map is disabled.

Example

```
Your Product(config-router)# distance 10 route-map rmap-test
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode.

clear ip bgp

Command Objective This command resets the BGP connection dynamically for inbound and outbound route policy. The inbound routing tables are updated dynamically or by generating new updates using stored update information.

If the keyword soft and the associated direction are not specified, then this causes hard clear, that is, the BGP session with peer is reset.

Syntax **clear ip bgp [vrf <string (32)>] {dampening [<random_str> <num_str>] | flap-statistics [<random_str> <num_str>] | { * | <AS no>| external | ipv4 | ipv6 | <random_str> } [soft [{in [prefix-filter]|out}]] }**

Parameter Description

- `vrf <vrf-name>` - Resets the BGP connection for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- `dampening [<random_str><num_str>]` - Clears the dampening related configuration for the bgp.
  - `<random_str>` - Clears damping information for the specified ipv4/ipv6 address.
  - `<num_str>` - Specifies the prefix length of the route. This value ranges between 0 and 128.
- `flap-statistics [<random_str> <num_str>` - Clears the route flap statistics for the bgp.
  - `<random_str>` - Clears flap statistics for the specified ipv4/ipv6 address.
  - `<num_str>` - Specifies the prefix length of the route. This value ranges between 0 and 128.
- ***** - Resets All BGP peers.
- `<AS no>` – Clear peers with the specified AS number. This value ranges between 1 and 4294967295 or 0.1 to 65535.65535.

  Notes:

  - When four-byte-asn is enabled, this value ranges between 0 and 4294967295or between 0.0 and 65535.65535
  - When four-byte-asn is disabled, this value ranges between 0 and 65535. or between 0.0 and 0.65535
  - When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.0 to 65535.65535
- `external` - Clear all external peers.
- `ipv4` - Resets the bgp connection dynamically for all ipv4 address family peers
- `ipv6` - Resets the bgp connection dynamically for all ipv6 address family peers
- `<random_str>` - Resets the bgp connection dynamically for the specified ip address or the configured peer group name.
  - `ip-address>` - Resets the bgp connection for the specified peer identified with the ip-address.
  - `<peer-group-name>` - Resets the bgp connection dynamically for all the members of the given peer group.
- `soft` - Configures the Soft clear which is automatically assumed when the route refresh capability is supported

- `in` - Initiates inbound soft reconfiguration which causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy
    - `prefix-filter` - Pushes out prefix-list ORF and initiates inbound soft reconfiguration
- `out` - Initiates outbound soft configuration which does not have any memory overhead and does not require any preconfiguration. An outbound reconfiguration can be triggered on the other side of the BGP session to make the new inbound policy take effect.

Mode Privileged EXEC Mode

Example `Your Product# clear ip bgp dampening 12.0.0.1 0`

Related Command(s)

- `bgp dampening` – Sets the BGP dampening parameters.
- `ip bgp dampening` - Configures the dampening parameters and changes various BGP route dampening factors.
- `show ip bgp` – Displays the BGP related information.
- `ip bgp four-byte-asn` - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system.
- `bgp asnotation dot` - Changes the output format of BGP ASNs from asplain to asdot notation.

do shutdown ip bgp

Command Objective This command sets the BGP Speaker Global Admin status DOWN.

The no form of the command sets the BGP Speaker Global Admin status UP. BGP functionally is active only when the global admin status is UP.

The shutdown command does not affect all the configurations. All peer sessions go down and routes learnt through redistribution are lost. If RFD is enabled, then routes history is cleared.

Syntax **do shutdown ip bgp [vrf <vrf-name>]**

no shutdown ip bgp [vrf <vrf-name>]

Parameter Description

- `vrf <vrf-name>` - Sets the BGP Speaker Global Admin status up / down for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32

Mode Global Configuration Mode

Default The BGP Speaker Global Admin status is DOWN.

Note: The BGP Speaker Global Admin status can be made UP only if the BGP Speaker Local

AS Number is configured.

Example Your Product(config)# do shutdown ip bgp

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `ip bgp overlap-policy` – Configures the Overlap Route policy for the BGP Speaker.
- `ip bgp synchronization / synchronization` – Enables synchronization between BGP and IGP.
- `show ip bgp info` – Displays the general information about BGP protocol.

debug ip bgp

Command Objective This command enables the tracing of the BGP module as per the configured debug levels. The trace statements are generated for the configured trace levels.

The no form of the command disables the tracing of the BGP module as per the configured debug levels. The trace statements are not generated for the configured trace levels.

Syntax **debug ip bgp [vrf <vrf-name>] [{all|ipv4 unicast |ipv6 unicast | <random_str>}] [{peer | update | fdb | keep | in | out | damp | events | gr }]**

no debug ip bgp [vrf <vrf-name>]{peer | update | fdb | keep | in | out | damp | events | gr | all}

Parameter Description

- `vrf <vrf-name>` - Generates debug ststements for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- `all` - Generates debug statements for all peers.
- `ipv4 unicast` - Generates debug statements for the trace code related to ipv4 peers or related ipv4 unicast address family peers.
- `ipv6 unicast` - Generates debug statements for the trace code related to ipv6 peers or related ipv6 unicast address family peers.
- `<random_str>` - Generates debug statements for the trace code related for the specified IPv4 or IPv6 peer address.
- `peer` - Generates debug statements forthe trace code related to peer processing.
- `update` - Generates debug statements for the trace code related to update processing
- `fdb` - Generates debug statements for the trace code related to FDB updation.
- `keep` - Generates debug statements for the trace code related to keep-alives.
- `in` - Generates debug statements for the trace code related to incoming messages.
- `out` - Generates debug statements for the Trace code related to outgoing messages.
- `damp` - Generates debug statements for the Trace code related to dampening parameters.
- `events` - Generates debug statements for the trace code related to BGP event processing.
- `gr` - Generates debug statements for the trace code related to graceful restart.
- `all` - Generates debug statements for all the BGP trace code.

Mode Privileged EXEC Mode

Note: This command executes only if BGP Speaker local AS number is configured.

Example `Your Product# debug ip bgp peer`

Related Command(s) `router bgp` – Sets the AS number of the BGP Speaker.

show bgp-version

Command Objective This command displays the BGP Version information.

Syntax **show bgp-version**

Mode Privileged EXEC Mode

Default The BGP Speaker Global Admin status is DOWN.

Example

```
Your Product# show bgp-version

BGP Version : 4
```

show ip bgp

Command Objective This command displays the BGP related information.

Syntax **show ip bgp [vrf <vrf-name>]{[neighbor [<peer-addr> [received prefix-filter]]]| [rib]| [stale]|[<ip_addr>] [prefix-len]}**

Parameter Description

- `vrf <vrf-name>` - Sets the BGP Speaker Global Admin status up / down for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- `neighbor <peer-addr>` - Displays BGP information for the specified IP address of the neighbor.
  - received prefix-filter - Displays the received ORF entries
- `rib` - Displays the BGP local RIB (Routing Information Base).
- `stale` - Displays the routes which have gone stale due to Graceful restart.
- `<ip addr>` - Displays BGP information for the specified IP address from the RIB.
- `prefix-len` - Displays BGP information for the specified prefix length from the RIB. This value ranges between 0 and 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp neighbor 60.0.0.5
BGP neighbor is 12.9.9.9, remote AS 23, external link
BGP version 0, remote router ID 0.0.0.0
BGP state = Idle
Configured BGP Maximum Prefix Limit 100
AutomaticStart DISABLED
AutomaticStop DISABLED
DampPeer Oscillations DISABLED
DelayOpen DISABLED
Configured Connect Retry Count 5
Current Connect Retry Count 0
Default-originate : DISABLED
Peer Passive : DISABLED
Peer Status : NOT DAMPED
GateWay Address : NONE
Rcvd update before 0 secs, hold time is 90, keepalive interval is 30 secs
Ip Prefix-list IN       : aa
Received 0 messages, 0 Updates
Sent 0 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 30 seconds
Connections established 0 time(s)
Local host: 12.0.0.2, Local port: 0
Foreign host: 12.9.9.9, Foreign port: 0
Last Error: Code 0, SubCode 0.
Update Source 12.0.0.2
Next-Hop is automatic
MultiHop Status - disabled
Send-Community is standard,extended
Your Product# show ip bgp rib
Context Name : default
--------------------
BGP table version is 1,local router ID is 60.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP,   e - EGP, ? - incomplete
Type                    Network  NextHop             Metric LocPrf Path
Origin
-------                 ------------  ------------          ---------- ---------- ------- --------
-
>                       66.0.0.0/8      60.0.0.66/4   0      -      ?
Your Product# show ip bgp stale
Context Name : default
--------------------
BGP table version is 7,local router ID is 60.0.0.5
Origin codes: i - IGP,   e - EGP, ? - incomplete
Network                 NextHop         Metric LocPrf Path Origin
--------                -------         ------ ------ ---- ------
66.0.0.0/8              60.0.0.66/4           100    200    ?
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `bgp router-id` – Configures the BGP Identifier of the BGP Speaker.

- neighbor - remote-as –Creates a Peer and initiates the connection to the peer.
- neighbor - interval – Configures neighbor interval.
- neighbor - timers– Configures neighbor KeepAlive Time and Hold Time Intervals.
- neighbor - shutdown – Disables the Peer session.
- neighbor - update-source - Configures the source-address for routing updates and for TCP connection establishment with a peer.
- neighbor - gateway - Configures gateway router's address that will be used as nexthop in the routes advertised to the peer.
- neighbor - activate – Enables default capabilities for the peer and restarts the connnection to the peer if capabilities negotiated change.
- neighbor - delay open - Configures a delay in sending the first OPEN message to the BGP peer for a specific time period.
- neighbor - maximum prefix - Configures the maximum number of eers supported by BGP.
- neighbor - damp-peer-oscillations - Enables the damp peer oscillation option.
- neighbor - allow-autostop - Enables the auto stop option to stop the BGP peer and BGP connection automatically.
- neighbor - connect-retrycount - Sets the retry count for the BGP peer.
- neighbor - transport connection-mode - Configures the BGP Peer Transport Connection status as active or passive.
- neighbor - peer-group – Creates a peer group.
- clear ip bgp–Resets the BGP connection dynamically for inbound and outbound route policy.
- neighbor - Local-as - Updates the local AS used for the peer connection.

show ip bgp restart mode

Command Objective This command displays the restart mode of the BGP router and neighbors.The BGP Speaker can be in restarting or receiving mode.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp {restartmode [neighbor [<peer-addr>]]}**

Parameter Description

- restartmode - Displays the restart mode fo the BGP router.
- neighbor <peer-addr> - Displays the restart mode for the specified IP address of the neighbor.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp restartmode neighbor 10.2.4.5
Context Name : default
---------------------
BGP4:- In Receiving Mode
```

```
Neighbor                RestartMode
---------------         ------------
                        None
Your Product# show ip bgp restartmode neighbor 23.45.0.1
Context Name : default
---------------------
BGP4:- Restart feature is not enabled Neighbor RestartMode
---------------         ------------
23.45.0.1 None Context Name : vrf1
---------------------
BGP4:- Restart feature is not enabled Context Name : vrf2
---------------------
BGP4:- Restart feature is not enabled
```

Related Command(s)

- `bgp graceful-restart` - Enables the graceful restart capability.
- `neighbor – remote-as` –Creates a Peer and initiates the connection to the peer.

show ip bgp EndOfRIBMarkerStatus

Command Objective This command displays the End_Of_RIB marker status of the BGP router and neighbors.

Syntax **show ip bgp [vrf <vrf-name>] {EndOfRIBMarkerStatus [neighbor [<peer-addr>]]}**

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Parameter Description

- `vrf <vrf-name>` - Displays the End_Of_RIB marker status for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- `neighbor <peer-addr>` - the End_Of_RIB marker status for the specified IP address of the neighbor.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp EndOfRIBMarkerStatus
Context Name : default
---------------------
Neighbor                     EORSent EORRcvd
-------------   ------------ ------------
60.0.0.5                  NA      Received
30.0.0.4    Sent    Received
Your Product# show ip bgp EndOfRIBMarkerStatus neighbor 60.0.0.5
Context Name : default
---------------------
Neighbor                     EORSent EORRcvd
-------------   ------------ ------------
```

```
60.0.0.5                  NA      Received
Your Product# show ip bgp vrf vrf1 EndOfRIBMarkerStatus
Context Name : vrf1
--------------------
Neighbor                     EORSent EORRcvd
-------------    ------------ ------------
23.45.0.1   NA       NA
```

Related Command(s) `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.

show ip bgp restartreason

Command Objective This command displays the restart reason of the BGP.

Syntax **show ip bgp restartreason**

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp restartreason
Context Name : default
--------------------
BGP4: Restart reason is software restart
Your Product# show ip bgp restartreason
Context Name : default
--------------------
BGP4: Restart reason is software upgrade
Your Product# show ip bgp restartreason
Context Name : vrf1
--------------------
BGP4: Restart reason is unknown
```

Related Command(s) `restart-reason` - Configures the reason for BGP graceful restart.

show ip bgp restartexitreason

Command Objective This command displays the restart exit reason of the BGP. This is the outcome of the last attempt at a graceful restart.

The valid exit reasons can be

- None – The speaker has not restarted.
- InProgress - A restart attempt is currently underway.
- Success- A restart is completed successfully.
- Failure - Failure due to the speaker is not completed the restart process within the restart interval.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp restartexitreason**

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp restartexitreason
Context Name : default
--------------------
BGP4: Restart In Progress
Your Product# show ip bgp restartexitreason
Context Name : default
--------------------
BGP4: Restart Speaker hs not restarted
Your Product# show ip bgp restartexitreason
Context Name : default
--------------------
BGP4: GR Exit Reason is Success
Your Product# show ip bgp restartexitreason
Context Name : default
--------------------
BGP4: GR Exit Reason is Failure
```

Related Command(s)

- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `bgp graceful-restart` - Enables the graceful restart capability.

show ip bgp restartsupport

Command Objective This command displays the restart support of the BGP.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp restartsupport**

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp restartsupport
BGP4: Both planned and unplanned restart are supported
Your Product# show ip bgp restartsupport
BGP4: Planned restart is supported
Your Product# show ip bgp restartsupport
BGP4: Speaker does not have restart support
```

Related Command(s)

- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `restart-support` - Enables the graceful restart support.

show ip bgp restartstatus

Command Objective This command displays the current restart status of the BGP. This indicates if the speaker is restarted or not and if it is restarted whether it is a planned restart or unplanned restart.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp restartstatus**

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp restartstatus
Context Name : default
--------------------
BGP4: Restart status in none
Context Name : vrf1
--------------------
BGP4: Restart status in unplanned
Context Name : vrf2
--------------------
BGP4: Restart status in none
```

Related Command(s)

- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `bgp graceful-restart` - Enables the graceful restart capability.

show ip bgp community-number

Command Objective This command displays routes that belong to specified BGP communities.

Syntax **show ip bgp community community-number(4294967041-4294967043,65536-4294901759) [exact]**

Note: To execute this command L3VPN flag should be enabled.

Parameter Description

- `community-number(4294967041-4294967043,65536-4294901759)` - Displays the routes that belong to the specified BGP Community attribute. This value ranges between 4294967041 and 4294967043 or between 65536 and 4294901759.
- `exact` - Displays the routes that has the same specified communities.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp community community-number 75000
BGP table version is 5,local router ID is 10.0.0.2
Status codes: d damped * valid, > best, I - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop    Metric LocPrf Path
-----------------------------------------    ----------   ----------- --------
76.0.0.0/8    10.0.0.1      1           100
77.0.0.0/8    10.0.0.1      1           100
78.0.0.0/8    10.0.0.1      1           100
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `bgp comm-route` – Configures an entry in additive or delete community table.

show ip bgp extcommunity – routes

Command Objective This command displays routes that belong to specified BGP extended-communities.

Syntax **show ip bgp extcommunity <value(xx:xx:xx:xx:xx:xx:xx:xx)> [exact]**

Note: To execute this command L3VPN flag should be enabled.

Parameter Description

- `<value(xx:xx:xx:xx:xx:xx:xx:xx)>` - Displays the routes for the specified extended community value. This is an octet string value in the form xx:xx:xx:xx:xx:xx:xx:xx.
- `exact` - Displays the routes that has the same specified extended communities.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp show ip bgp extcommunity 01:02:33:33:33:33:33:33
BGP table version is 5,local router ID is 10.0.0.2
Status codes: d damped * valid, > best, I - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop    Metric LocPrf Path
-----------------------------------------    ----------   ----------- --------
75.0.0.0/8    10.0.0.1      1           100
79.0.0.0/8    10.0.0.1      1           100
Your Product# show ip bgp extcommunity 01:02:33:33:33:33:33:33 exact
BGP table version is 5,local router ID is 10.0.0.2
Status codes: d damped * valid, > best, I - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop    Metric LocPrf Path
------------      ---------------   --------  ---------- -------
75.0.0.0/8   10.0.0.1      1           100
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `bgp ecomm-route` – Configures an entry in additive or delete extended community table.

show ip bgp summary

Command Objective This command displays the status of all BGP4 connections. If the VRF option is specified it displays the status of BGP4 connection for the specified VRF instance.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp summary [vrf <vrf-name>]**

Parameter Description

- `vrf <vrf-name>` - Displays the status of BGP4 connections for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp summary
Context Name : default
--------------------
BGP router identifier is 12.0.0.1, local AS number 1 Forwarding State is enabled
BGP router identifier is 12.0.0.1, local AS number 1
BGP table version is 0
Neighbor    Version    AS    MsgRcvd  MsgSent   Up/Down State/PfxRcd
--------------  ------------  ---   -----------  -----------   -----------
----------------------
23.45.0.1    4         66       0        0           -
Idle
Context Name : vrf1
--------------------
BGP router identifier is 0.0.0.0, local AS number 1 Forwarding State is enabled
BGP router identifier is 0.0.0.1, local AS number 1

BGP table version is 0
Neighbor    Version    AS    MsgRcvd  MsgSent   Up/Down State/PfxRcd
--------------  ------------  ---   -----------  -----------   -----------
----------------------
Context Name : vrf2
--------------------
BGP router identifier is 0.0.0.0, local AS number 1 Forwarding State is enabled
BGP router identifier is 0.0.0.1, local AS number 1
BGP table version is 0
Neighbor    Version    AS    MsgRcvd  MsgSent   Up/Down State/PfxRcd
--------------  ------------  ---   -----------  -----------   -----------
----------------------
```

```
Your Product# show ip bgp summary vrf default
Context Name : default
--------------------
BGP router identifier is 12.0.0.1, local AS number 1 Forwarding State is enabled
BGP router identifier is 12.0.0.1, local AS number 1
BGP table version is 0
Neighbor    Version    AS     MsgRcvd  MsgSent   Up/Down State/PfxRcd
--------------   ------------   ---     -----------  -----------    -----------
----------------------
23.45.0.1    4          66       0        0          -
Idle
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `bgp router-id` – Configures the BGP Identifier of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.

show ip bgp filters

Command Objective This command displays the contents of filter table.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp filters [vrf <vrf-name>]**

Parameter Description

- vrf <vrf-name> - Displays the contents of filter table.for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp filters
Context Name : default
--------------------
Index AdminStatus Remote-AS Prefix PrefixLen Inter-AS  Direction Action
-------- ----------------- -------------- ---------- -------------- ------------ -----
6       up          145     72.93.0.0 16        150      in    filter
```

```
Context Name : vrf1
--------------------
Index AdminStatus Remote-AS Prefix                PrefixLen Inter-AS  Direction Action
-------- ----------------- -------------- ------------------------------- ------------ ------------ -------------- --------
Your Product# show ip bgp filters vrf default
Context Name : default
--------------------
```

```
Index AdminStatus Remote-AS Prefix PrefixLen Inter-AS  Direction Action
-------- ------------------ -------------- ---------- -------------- ------------- -----
6       up          145     72.93.0.0 16       150      in    filter
```

Related Command(s) `bgp update-filter` – Configures an entry in Update Filter Table.

show ip bgp aggregate

Command Objective This command displays the contents of aggregate table.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp aggregate [vrf <vrf-name>]**

Parameter Description

- `vrf <vrf-name>` - Displays the contents of the aggregate table.for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp aggregate
Context Name : default
------------------------------------
Index AdminStatus   Prefix PrefixLen Advertise
--------- ---------------------- --------------------------- ---------------------------
1       up            10.0.0.0    8     all
2       up            20.0.0.0    8     summary-only
3       up            50.0.0.0    8     all
```

Related Command(s) `aggregate-address index` – Configures an entry in Aggregate Table.

show ip bgp med

Command Objective This command displays the contents of MED table.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp med [vrf <vrf-name>]**

Parameter Description

- vrf <vrf-name> - Displays the contents of MED table.for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp med
Context Name : default
--------------------
Index Admin  Remote-AS Prefix PrefixLen Inter-AS  Direction Value PreferenceStatus
----------- -------------- ---------- -------------- ------------ --------------
-------------------
5       up         200    212.23.45.0 24       150    in
50   true
Context Name : vrf1
--------------------
Index Admin  Remote-AS Prefix PrefixLen Inter-AS  Direction Value PreferenceStatus
----------- -------------- ---------- -------------- ------------ --------------
-------------------
Your Product# show ip bgp med default
Context Name : default
--------------------
Index Admin  Remote-AS Prefix PrefixLen Inter-AS  Direction Value PreferenceStatus
----------- -------------- ---------- -------------- ------------ --------------
-------------------
5       up         200    212.23.45.0 24       150    in
50   true
```

Related Command(s)

- `bgp med` – Configures an entry in MED Table.
- `bgp bestpath med confed` – Enables MED comparison among paths learnt from confed peers

show ip bgp dampening

Command Objective This command displays the contents of Dampening table.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp dampening [vrf <vrf-name>] [{flap-statistics | dampened-paths}]**

Parameter Description

- `vrf <vrf-name>` - Displays the contents of Dampening table for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- `flap-statistics` - Displays the flap-statistics contents of Dampening table.
- `dampened-paths` - Displays the dampened-paths contents of Dampening table.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp dampening
Context Name : default
----------------------
Half Life Time is 900
Reuse value is 750
Suppress value is 2000
Max Suppress time is 3600
Decay timer granularity is 1
Reuse timer granularity is 15
Reuse index array size is 1024
Context Name : vrf1
----------------------
Half Life Time is 1000
Reuse value is 1998
Suppress value is 2000
Max Suppress time is 3600
Decay timer granularity is 1
Reuse timer granularity is 135
Reuse index array size is 257
Context Name : vrf2
----------------------
Half Life Time is 2000
Reuse value is 1990
Suppress value is 2050
Max Suppress time is 3600
Decay timer granularity is 1
Reuse timer granularity is 135
Reuse index array size is 257
Your Product# show ip bgp dampening vrf default
Context Name : default
----------------------
Half Life Time is 601
Reuse value is 750
Suppress value is 2000
Max Suppress time is 3600
Decay timer granularity is 1
Reuse timer granularity is 15
Reuse index array size is 1024
Your Product# show ip bgp dampening flap-statistics
Context Name : default
----------------------
BGP table version is 3,local router ID is 12.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Type   Network  NextHop   Flaps Duration   Reuse  Path  Origin
-------  ------------  ------------  --------  ----------   ------------- -------  --------
> 40.0.0.0/8  12.0.0.1  1  00:00:4:8    -        100    ?
Your Product# show ip bgp dampening dampened-paths
Context Name : default
----------------------
BGP table version is 3,local router ID is 12.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Type   Network   NextHop     Reuse         Path        Origin
```

```
h    40.0.0.0/8    12.0.0.1      00:1:40:45         100     ?
```

Related Command(s)

- `ip bgp dampening` – Configures the Dampening Parameters.
- `bgp dampening` – Configures the Dampening Parameters.

show ip local-pref

Command Objective This command displays the contents of local preference table.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp local-pref [vrf <vrf-name>]**

Parameter Description

- `vrf <vrf-name>` - Displays the contents of local preference table.for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp local-pref
Context Name : default
----------------------
Cluster id is           12.0.0.1
Desired Support of the route reflector - Client Support BGP Peer Extension Table
Peer Address Client/Non-Client
------- ----------- ---------------------------
13.0.0.25    Non-Client
Context Name : vrf1
----------------------
Cluster id is           None
Desired Support of the route reflector - Client Support BGP Peer Extension Table
Peer Address Client/Non-Client
------- ----------- ---------------------------
25.0.0.25    Non-Client
Your Product# show ip bgp local-pref vrf default
Context Name : default
--------------------
Cluster id is           12.0.0.1
Desired Support of the route reflector - Client Support
BGP Peer Extension Table
Peer Address Client/Non-Client
------- ----------- ---------------------------
13.0.0.25    Non-Client
```

Related Command(s) `bgp local-preference` – Configures an entry in Local Preference Table.

show ip bgp timers

Command Objective This command displays the value of BGP timers.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp timers [vrf <vrf-name>]**

Parameter Description

- `vrf <vrf-name>` - Displays the value of BGP timers for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp timers
Context Name : default
--------------------
Graceful restart Timers
---------------------------------------
Restart Time             90
Stale Time               150
Selection Deferral Timer Time       60
Peer Timers
Peer Address Holdtime KeepAliveTime ConnectRetry
ASOrig IdleHoldTime DelayOpenTime RouteAdvt RestartTime
                            ------- ----------- ------------ ------------- ------------- --------
                          ------------- ------------- ---------- -------------
23.45.0.1        90       30             30        15             60                0
30       NA
Context Name : vrf1
--------------------
Graceful restart Timers
---------------------------------------
Restart Time             90
Stale Time               150
Selection Deferral Timer Time       60
Peer Timers
Peer Address Holdtime KeepAliveTime ConnectRetry
ASOrig IdleHoldTime DelayOpenTime RouteAdvt RestartTime
                            ------- ----------- ------------ ------------- ------------- --------
                          ------------- ------------- ---------- -------------
Context Name : vrf2
--------------------
Graceful restart Timers
---------------------------------------
Restart Time             90
Stale Time               150
Selection Deferral Timer Time       60
```

```
Peer Timers
Peer Address Holdtime KeepAliveTime ConnectRetry
ASOrig IdleHoldTime DelayOpenTime RouteAdvt RestartTime
                            ------- ----------- ------------ ------------------------------ -------------------- --------
                          ------------------- -------------------- -------------- --------------------

                        Your Product# show ip bgp timers vrf default
Context Name : default
-------------
Graceful restart Timers
-------------------------
Restart Time            90
Stale Time              150
Selection Deferral Timer Time       60
Peer Timers
Peer Address Holdtime KeepAliveTime ConnectRetry
ASOrig IdleHoldTime DelayOpenTime RouteAdvt RestartTime
                            ------- ----------- ------------ ------------------------------ -------------------- --------
                          ------------------- -------------------- -------------- --------------------

23.45.0.1        90      30             30       15             60               0
30       NA
```

Related Command(s)

- `ip bgp dampening` – Configures the Dampening Parameters.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - interval` – Configures neighbor interval.
- `neighbor - timers` – Configures neighbor KeepAlive Time and Hold Time Intervals.
- `neighbor - peer-group` – Creates a peer group.
- `bgp graceful-restart` - Enables the graceful restart capability.
- `bgp update-delay` - Configures the selection deferral time interval.

show ip bgp info

Command Objective This command displays the general information about BGP protocol.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp info [vrf <vrf-name>]**

Parameter Description

- `vrf <vrf-name>` - Displays the general information about BGP protocol for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp info
Context Name : default
--------------------
Routing Protocol is "bgp 1" Bgp Trap : Enabled
The route change interval is "60" IGP synchronization is enabled
Both more-specific and less-specific overlap route policy is set
Administrative Distance is 122
Default IPv4 Unicast Capability Status is set
Local Preference is 100
Non-bgp routes are advertised to bothexternal and internal peers
MED Comparision is disabled
Metric is 0
Default Originate Disable
Redistributing:
BGP GR admin status is disabled
Maximum paths: ibgp - 1 ebgp -   1 eibgp - 64
Maximum paths (Operational): ibgp - 1 ebgp -   1 eibgp - 1
Peer Table
Peer Address RemoteAS NextHop   MultiHop  Send-community
                        ------- ----------- ------------ ----------- ------------ ------------------------------
                         23.45.0.1    66     self       enable    standard,extended
Context Name : vrf1
--------------------
Routing Protocol is "bgp 1"
Bgp Trap : Enabled
The route change interval is "60"
IGP synchronization is enabled
Both more-specific overlap route policy is set
Administrative Distance is 122
Default IPv4 Unicast Capability Status is set
Local Preference is 100
Non-bgp routes are advertised to bothexternal and internal peers
MED Comparision is disabled
Metric is 0
Default Originate Enable
Redistributing:
BGP GR admin status is disabled
Maximum paths: ibgp - 1 ebgp -   1 eibgp - 64
Maximum paths (Operational): ibgp - 1 ebgp -   1 eibgp - 1
Peer Table
                        Peer Address RemoteAS NextHop   MultiHop  Send-community
                         ------- ----------- ------------ ----------- ------------ ------------------------------
Context Name : vrf2
--------------------
Routing Protocol is "bgp 1"
Bgp Trap : Enabled
The route change interval is "60"
IGP synchronization is enabled
Both more-specific overlap route policy is set
Administrative Distance is 122
Default IPv4 Unicast Capability Status is set
Local Preference is 100
Non-bgp routes are advertised to bothexternal and internal peers
MED Comparision is disabled
Metric is 0
```

```
Default Originate Enable
Redistributing:
BGP GR admin status is disabled
Maximum paths: ibgp - 1 ebgp -    1 eibgp - 64
Maximum paths (Operational): ibgp - 1 ebgp -   1 eibgp - 1
Peer Table
                        Peer Address RemoteAS NextHop   MultiHop  Send-community
                         ------- ----------- ------------ ----------- ------------ ------------------------------
Your Product# show ip bgp info vrf default
Context Name : default
--------------------
Routing Protocol is "bgp 1" Bgp Trap : Enabled
The route change interval is "60" IGP synchronization is disabled
More-specific overlap route policy is set
Administrative Distance is 122
Default IPv4 Unicast Capability Status is set
Local Preference is 100
Non-bgp routes are advertised to bothexternal and internal peers
MED Comparision is disabled
Metric is 0
Default Originate Disable
Redistributing:
BGP GR admin status is disabled
Maximum paths: ibgp - 1 ebgp -    1 eibgp - 64
Maximum paths (Operational): ibgp - 1 ebgp -   1 eibgp - 1
Peer Table
                        Peer Address RemoteAS NextHop   MultiHop  Send-community
                         ------- ----------- ------------ ----------- ------------ ------------------------------
                         60.0.0.5      500      automatic disable standard,extended
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `ip bgp overlap-policy` – Configures the Overlap Route policy for the BGP Speaker.
- `default-information originate` - enables redistribution and advertisement of the default router.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `ip bgp synchronization / synchronization` – Enables synchronization between BGP and IGP.
- `bgp default local-preference` – Configures the Default Local Preference value.
- `neighbor - ebgp-multihop` – Enables BGP to establish connection with external peers.
- `neighbor - next-hop-self` – Enables BGP to send itself as the next hop for advertised routes.
- `neighbor - interval` – Configures neighbor interval r.
- `neighbor - activate` – Enables default capabilities for the peer and restarts the connnection to the peer if capabilities negotiated change.
- `neighbor - send-community` – Enables advertisement of community attributes to (standard/extended) peer.
- `neighbor - timers` – Configures neighbor KeepAlive Time and Hold Time Intervals.
- `bgp nonbgproute-advt` – Controls the advertisement of Non-BGP routes.
- `redistribute` – Configures the protocol from which the routes have to be redistributed into BGP.

- `bgp always-compare-med` – Enables the comparison of med for routes received from different autonomous system.
- `default-metric` – Configures the Default IGP Metric value
- `neighbor - password` – Configures the password for TCP-MD5 authentication with peer.
- `bgp graceful-restart` - Enables the graceful restart capability.
- `do shutdown ip bgp` – Sets the BGP Speaker Global Admin status DOWN..
- `bgp trap` - Enables /disables the bgp trap notification.
- `nexthop processing-interval` - Configures the interval at which next hops are monitored for reachablity.
- `redistribute ospf` - Configures the OSPF protocol from which the routes are redistributed into BGP.
- `maximum-paths` - Sets the BGP multipath count.

show ip rfl info

Command Objective This command displays information about Route Reflector feature.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp rfl info [vrf <vrf-name>]**

Parameter Description

- `vrf <vrf-name>` - Displays the information about Route Reflector feature for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp rfl info
Context Name : default
----------------------
Cluster id is           12.0.0.1
Desired Support of the route reflector - Client Support BGP Peer Extension Table
Peer Address Client/Non-Client
------- ----------- ---------------------------
23.45.0.1      Non-Client
Context Name : vrf1
----------------------
Cluster id is           None
Desired Support of the route reflector - Client Support BGP Peer Extension Table
Peer Address Client/Non-Client
------- ----------- ---------------------------
Your Product# show ip bgp rfl info vrf default
Context Name : default
----------------------
Cluster id is           12.0.0.1
```

```
Desired Support of the route reflector - Client Support
BGP Peer Extension Table
Peer Address Client/Non-Client
------- ------------ ----------------------------
23.45.0.1     Non-Client
```

Related Command(s)

- `bgp nonbgproute-advt` – Controls the advertisement of Non-BGP routes either to the external peer (1) or both to internal & external peer (2)
- `bgp client-to-client reflection` – Configures the Route Reflector to support route reflection to Client Peers.
- `neighbor - route-reflector-client` – Configures the Peer as Client of the Route Reflector.
- `bgp cluster-id` – Configures the Cluster ID for Route Reflector.

show ip bgp confed info

Command Objective This command displays information about confederation feature.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp confed info [vrf <vrf-name>]**

Parameter Description

- `vrf <vrf-name>` - Displays the information about confederation feature for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp confed info
Context Name : default
----------------------
Confederation Identifier is 1000
Confederation best path med comparision is set
Confederation peers: 100
Context Name: vrf1
----------------------
Confederation Identifier is 0
Confederation best path med comparision is not set
Confederation peers: None
Context Name: vrf2
----------------------
Confederation Identifier is 0
Confederation best path med comparision is not set
Confederation peers: None
Your Product# show ip bgp confed info vrf default
Context Name : default
----------------------
```

```
Confederation Identifier is 1000
Confederation best path med comparision is set
Confederation peers: 100
```

Related Command(s)

- `bgp confederation identifier` – Configures the BGP confederation identifier.
- `bgp bestpath med confed` – Enables MED comparison among paths learnt from confed peers.
- `bgp confederation peers` – Configures the Autonomous Systems that belongs to the confederation.

show ip bgp community

Command Objective This command displays the contents of community tables.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp community [vrf <vrf-name>] {route|policy|filter}**

Parameter Description

- `vrf <vrf-name>` - Displays contents of community tables for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- `route` - Displays the entry in additive or delete community table.
- `policy` - Displays the Community attribute advertisement policy for specific destination.
- `filter` - Displays the filter community attribute while receiving or advertising.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp community route
Context Name : default
-----------------------------------
Additive  Community Table
Prefix                            PrefixLen    AddCommVal
------------------------------------------------------------------------------------
30.0.0.0        8         70000
60.0.0.0        8         75000
75.0.0.0        8         70000
76.0.0.0        8         75000
77.0.0.0        8         75000
78.0.0.0        8         75000
78.0.0.0        8         76000
Delete Community Table
Prefix                            PrefixLen    DeleteCommVal
---------         -----------------     ------------------------
40.0.0.0        8         80000
70.0.0.0        8         85000
Your Product# show ip bgp community filter
--------------------------
```

```
Context Name : default
Incoming Filter Table
CommValue    FilterStatus
--------------  --------------------
70000       accept
80000       deny
Outgoing Filter Table
CommValue    FilterStatus
--------------  --------------------
75000       accept
80000       deny
Your Product# show ip bgp community policy
Context Name : default
----------------------
Community Policy Table
Prefix                            PrefixLen    SendStatus
--------        --------------    ---------------
20.0.0.0        8          set-add
30.0.0.0        8          set-none
40.0.0.0        8          modify
```

Related Command(s)

- `bgp comm-route` – Configures an entry in additive or delete community table.
- `bgp comm-filter` – Allows/filters the community attribute while receiving or advertising.
- `bgp comm-policy` – Configures the community attribute advertisement policy for specific destination.

show ip bgp extcommunity

Command Objective This command displays the contents of extended -community tables.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp [vrf <vrf-name>] extcommunity {route|policy|filter}**

Parameter Description

- `vrf <vrf-name>` - Displays the contents of extended -community tables for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- `route` - Displays the entry in additive or delete ext community table.
- `policy` - Displays the extended community attribute advertisement policy for specific destination.
- `filter` - Displays the extended community filters attribute while receiving or advertising.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp extcommunity route
-------------------------
```

```
Context Name : default
Additive Ext-Community Table
Prefix                           PrefixLen    AddECommVal
--------------------------------------    ----------------------------------------
30.0.0.0        8          1:1:22:33:44:55:66:77
60.0.0.0        8          1:1:22:33:44:55:66:88
75.0.0.0        8          1:1:33:33:33:33:33:33
76.0.0.0        8          1:2:44:33:33:33:33:33
78.0.0.0        8          1:2:33:33:33:33:33:33
78.0.0.0        8          1:2:33:33:33:33:33:44
79.0.0.0        8          1:2:33:33:33:33:33:44
79.0.0.0        8          1:2:33:33:33:33:33:33
Delete Ext-Community Table
Prefix                           PrefixLen    DeleteECommVal
--------------------------------------    -----------------------
40.0.0.0        8         80000
70.0.0.0        8         85000
Context Name : vrf1
-----------------------
Additive Ext-Community Table
Prefix                           PrefixLen    AddECommVal
--------        ---------------    -------------------
Delete Ext-Community Table
Prefix                           PrefixLen    DeleteECommVal
Your Product# show ip bgp extcommunity filter
Context Name : default
-----------------------
Incoming Filter Table
EcommValue                                FilterStatus
---------                -------------
1:1:22:33:44:55:34:77     deny
1:1:22:33:44:55:66:77     accept
Outgoing Filter Table
EcommValue                            FilterStatus
---------               -------------
1:1:22:33:44:55:99:77    accept
1:1:44:33:77:66:99:56    deny
Your Product# show ip bgp extcommunity policy
Context Name : default
-----------------------
Ecommunity Policy Table
Prefix                           PrefixLen    SendStatus
--------        ---------------    ----------------
20.0.0.0        8         set-add
30.0.0.0        8         set-none
40.0.0.0        8         modify
```

Related Command(s)

- `bgp ecomm-route` – Configures an entry in additive or delete ext community table.
- `bgp ecomm-filter` – Allows/filters the ext community attribute while receiving or advertising.
- `bgp ecomm-policy` – Configures the extended community attribute advertisement policy for specific destination.

neighbor – maximum-prefix

Command Objective This command configures the maximum number of peers supported by BGP. BGP speaker imposes a locally-configured, upper bound on the number of address prefixes the speaker is willing to accept from a neighbor.

The no form of the command resets the max number of routes that is learned from that particular peer.

Syntax **neighbor <ip-address|peer-group-name> maximum-prefix <prefix-limit>**

no neighbor <ip-address|peer-group-name> maximum-prefix

Parameter Description

- `<ip-address>` - Configures the remote BGP peer IP address for which the maximum peer is to be set.
- `<peer-group-name>` - Specifies the name of the BGP peer group for which the maximum peer is to be set. The members of the peer group will inherit the characteristic configured with this command.
- `maximum-prefix <prefix-limit>` - Configures the maximum number of address prefixes that the BGP Peer is willing to accept from the neighbor. This value ranges between 1 and 5000.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 100

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example
```
Your Product(config-router)# neighbor 23.45.0.1 maximum-prefix 255
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor` - remote-as – Creates a Peer and initiates the connection to the peer.
- `neighbor` - peer-group – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

neighbor – connect-retry-count

Command Objective This command sets the retry count for the BGP peer. This counter denotes the number of times the BGP Peer should try to establish a TCP-Connect issue with its neighboring peers. The default value for the counter is set as 5. If the BGP Peer exceeds the maximum count value, automatic stop event takes place and the BGP Peer is brought down to the Idle State.

The no form of the command resets the retry count of the BGP peer.

Syntax **neighbor <ip-address|peer-group-name> connect-retry-count <value(1-50)>**

no neighbor <ip-address|peer-group-name> connect-retry-count

Parameter Description

- `<ip-address>` - Configures the remote IP address of the BGP peer for which the retry count is to be set.
- `<peer-group-name>` - Specifies the name of the BGP peer group for which the retry count is to be set. The members of the peer group will inherit the characteristic configured with this command.
- `connect-retry-count <value(1-50)>` - Configures the retry count which specifies the number of times the BGP peer should try to establish a TCP-connect issue with its neighboring peers. If the BGP Peer exceeds the maximum count value, automatic stop event takes place and the BGP Peer is brought down to the Idle State. This value ranges between 1 and 50.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 5

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 12.0.0.1 connect-retry-count 50
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.
- `as-num` - Sets the AS (Autonomous System) number for the router.
- `router-id` - Sets the router ID’s address for the router.

neighbor – allow-autostop

Command Objective This command enables the auto stop option to stop the BGP peer and BGP connection automatically.

The no form of this command disables the auto stop option.

Syntax **neighbor <ip-address|peer-group-name> allow-autostop**

no neighbor <ip-address|peer-group-name> allow-autostop

Parameter Description

- `<ip-address>` - Configures the remote IP address of the BGP peer for which the auto stop option is set.

- `<peer-group-name>` - Specifies the name of the BGP peer group for which the auto stop option is set. The members of the peer group will inherit the characteristic configured with this command.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Auto stop option is disbaled.

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 12.0.0.1 allow-autostop
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

neighbor - damp-peer-oscillations

Command Objective This command enables the damp peer oscillation option On implementing this logic, it damps the oscillations of BGP peers in the face of sequences of automatic start and automatic stop in the IDLE state.

The no form of this commnd disables the damp peer oscillation option.

Syntax **neighbor <ip-address|peer-group-name> damp-peer-oscillations**

no neighbor <ip-address|peer-group-name> damp-peer-oscillations

Parameter Description

- `<ip-address>` - Configures the remote IP address of the BGP peer for which the damp peer oscillation option is set.
- `<peer-group-name>` - Specifies the name of the BGP peer group for which the damp peer oscillation option is set. The members of the peer group will inherit the characteristic configured with this command.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Damp peer oscillation option is disbaled.

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 12.0.0.1 damp-peer-oscillations
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

neighbor delay-open

Command Objective This command configures a delay in sending the first OPEN message to the BGP peer for a specific time period.

The no form of the command disables the delay open option.

Syntax **neighbor <ip-address|peer-group-name> delay-open**

no neighbor <ip-address|peer-group-name> delay-open

Parameter Description

- `<ip-address>` - Configures the remote IP address of the BGP peer for which the delay open option is set.
- `<peer-group-name>` - Specifies the name of the BGP peer group for which the delay open option is set. The members of the peer group will inherit the characteristic configured with this command.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Delay open option is disbaled.

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 12.0.0.1 delay-open
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

bgp trap

Command Objective This command enables or disables the bgp trap notification.

Syntax **bgp trap <enable|disable>**

Parameter Description

- `enable` - Enables the trap notification for the BGP system. When there is any change in the graceful restart state of the router or peer, the BGP system sends the notification messages to the SNMP manager. For every graceful restart, appropriate trace messages is generated.
- `disable` - Disables the trap notification for the BGP system and does not send the notification messages to the SNMP manager.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default enable.

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product (config-router)# bgp trap enable
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp info` – Displays the general information about BGP protocol.

neighbor – peer group

Command Objective This command creates a peer group with the specified peer group name.This value is a string with the maximum size as 20.

The no form of the command deletes the peer group.

Syntax **neighbor <peer-group-name> peer-group**

no neighbor <peer-group-name> peer-group

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Delay open option is disbaled.

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor a1 peer-group
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.

- neighbor <ip-address> peer-group – Adds the neighbor as a member of the specified peer group.
- neighbor - activate – Enables default capabilities for the peer and restarts the connnection to the peer if capabilities negotiated change.
- neighbor - ebgp-multihop – Enables BGP to establish connection with external peers.
- neighbor - next-hop-self – Enables BGP to send itself as the next hop for advertised routes.
- neighbor - interval – Configures neighbor interval.
- neighbor - timers– Configures neighbor KeepAlive Time and Hold Time Intervals.
- neighbor - shutdown – Disables the Peer session.
- neighbor - default-originate - Enables advertisement of the default route to the peer.
- neighbor - send-community – Enables advertisement of community attributes to (standard/extended) to peer.
- neighbor - capability - Enables the specific BGP capability to be advertised and received from the peer.
- neighbor delay open - Configures a delay in sending the first OPEN message to the BGP peer for a specific time period.
- neighbor damp-peer-oscillations - Enables the damp peer oscillation option.
- neighbor maximum prefix - Configures the maximum number of peers supported by BGP.
- neighbor - allow-autostop - Enables the auto stop option to stop the BGP peer and BGP connection automatically.
- neighbor - transport connection-mode - Configures the BGP Peer Transport Connection status as active or passive.
- neighbor - connect-retrycount - Sets the retry count for the BGP peer.
- show ip bgp peer-group – Displays information abouty the peer group.
- address-family - Enters the router into the address-family router configuration mode.

neighbor delay-open

Command Objective This command configures a delay in sending the first OPEN message to the BGP peer for a specific time period.

The no form of the command disables the delay open option.

Syntax **neighbor <ip-address|peer-group-name> delay-open**

no neighbor <ip-address|peer-group-name> delay-open

Parameter Description

- <ip-address> - Configures the remote IP address of the BGP peer for which the delay open option is set.
- <peer-group-name> - Specifies the name of the BGP peer group for which the delay open option is set. The members of the peer group will inherit the characteristic configured with this command.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Delay open option is disbaled.

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example `Your Product(config-router)# neighbor 12.0.0.1 delay-open`

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

neighbor <ip-address> peer-group

Command Objective This command configures a delay in sending the first OPEN message to the BGP peer for a specific time period.

The no form of the command disables the delay open option.

Syntax **neighbor <ip-address> peer-group <peer-group-name>**

no neighbor <ip-address> peer-group <peer-group-name>

Parameter Description

- `<ip-address>` - Specifies the IP address of the peer/ neighbor to be added/ removed from the peer group.
- `<peer-group-name>` - Specifies the peer groujp name to which the neighbor is to be added/ removed.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Note: This command executes only if

- Peer is created and Peer AS is configured.
- Peer Group is created.

Example `Your Product(config-router)# neighbor 10.3.4.5 peer-group a1`

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.

- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

neighbor – routemap

Command Objective This command enables routemap or IP prefix list for the neighbor.

The no form of the command disables routemap or IP prefix list for the neighbor.

Syntax **neighbor <ip-address|peer-group-name> { route-map <name(1-20)> | prefix-list <ipprefixlist_name(1-20)>} {in | out}**

no neighbor <ip-address|peer-group-name> { route-map <name(1-20)> | prefix-list <ipprefixlist_name(1-20)>} {in | out}

Parameter Description

- `<ip-address>` - Enables/ Disables Routemap or IP Prefix List for the specified BGP peer's remote IP address.
- `<peer-group-name>` - Enables/ Disables Routemap for the specified BGP peer group. This value is a string with the maximum size as 20.
- `route-map <name(1-20)>` - Specifies the name of the Route Map. This value is a string with the maximum size as 20.
- `prefix-list <ipprefixlist_name>` - Configures IP prefix list for neighbor. This value is a string with the maximum size as 20.
- `in` - Enables/ Disables Routemap or IP Prefix List for inbound routes.
- `out` - Enables/ Disables Routemap or IP Prefix List for outbound routes.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Note: This command executes only if Peer/ Peer Group is created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 10.3.4.5 route-map r1 in
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

neighbor - transport connection-mode

Command Objective This command configures the BGP Peer Transport Connection status as active or passive.

Syntax **neighbor <ip-address|peer-group-name> transport connection-mode <active | passive>**

Parameter Description

- `<ip-address>` - Configures the transport connection status for the specified BGP peer's remote IP address.
- `<peer-group-name>` - Specifies name of the BGP peer group for which the transport connection mode is set. The members of the peer group will inherit the characteristic configured with this command.
- `active` - Sets the BGP peer as active. When a peer transport connection is made active, then the peer will immediately initiate the session with the peer by sending an open message to it.
- `passive` - Sets the BGP peer as passive. When the peer transport connection is passive, then the peer will not immediately initiate the session, instead, it waits for the peer to send the open message so that it can respond to it to create the session.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Auto stop option is disbaled.

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 12.0.0.1 allow-autostop
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

nexthop processing-interval

Command Objective This command configures the interval at which next hops are monitored for reachablity. This value ranges between 1 and 120.

Syntax nexthop processing-interval <Next-Hop-Processing-Interval(1-120)>

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 60

Example Your Product(config)# nexthop processing-interval 100

Related Command(s)

- router bgp – Sets the AS number of the BGP Speaker.
- address-family - Enters the router into the address-family router configuration mode.
- show ip bgp info – Displays the general info about BGP protocol.

bgp redistribute internal

Command Objective This command enables IBGP routes to be redistributed to other IGP protocols.

The no form of the command disables IBGP routes to be redistributed to other IGP protocols.

Syntax **bgp redistribute-internal**

no bgp redistribute-internal

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default IBGP route redistribution is disabled

Example Your Product(config-router)# bgp redistribute-internal

Related Command(s)

- router bgp – Sets the AS number of the BGP Speaker.
- show ip bgp info – Displays the general info about BGP protocol.

show ip bgp peer-group

Command Objective This command displays information about the peer group.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp [vrf <vrf-name>] peer-group [<peer-group-name> [summary]]**

Parameter Description

- vrf <vrf-name> - Displays information about the peer group for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- <peer-group-name> - Displays information for the specified BGP Peer group.
- summary - Dsiplays the summary of the peer group neighbors.

Mode Privileged EXEC Mode

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product# show ip bgp peer-group
Context Name : default
--------------------
BGP peer-group is a1, Remote AS 1 BGP Version 0
For address family: IPv4 Unicast
BGP neighbor is a1,peer-group internal, members: 12.3.3.3
BGP Maximum Prefix Limit: 2
Connect Retry Count: 2
Peer Passive :Enabled
Damp Peer oscillatios:Enabled Rfl Status :Non Client
In Route Map: n1
Out Route Map: -
Your Product# show ip bgp peer-group summary
Context Name : default
--------------------
BGP router identifier is 12.0.0.2, local AS number 1
Forwarding State is enabled
BGP table version is 0
Neighbor  Version  AS  MsgRcvd  MsgSent  Up/Down  State/PfxRcd
--------------- ------------ ---- ------------ ------------ ------------ --------------------
12.3.3.3    4        1         0         0        -       Connect
```

Related Command(s)

- `neighbor <ip-address> peer-group` – Adds the neighbor as a member of the specified peer group.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `neighbor - activate` – Enables default capabilities for the peer and restarts the connnection to the peer if capabilities negotiated change
- `neighbor - ebgp-multihop` – Enables BGP to establish connection with external peers.
- `neighbor - next-hop-self` – Enables BGP to send itself as the next hop for advertised routes.
- `neighbor - shutdown` – Disables the Peer session.
- `neighbor delay open` - Configures a delay in sending the first OPEN message to the BGP peer for a specific time period.
- `neighbor damp-peer-oscillations` - Enables the damp peer oscillation option.
- `neighbor maximum prefix` - Configures the maximum number of peers supported by BGP.
- `neighbor – allow-autostop` - Enables the auto stop option to stop the BGP peer and BGP connection automatically.
- `neighbor – transport connection-mode` - Configures the BGP Peer Transport Connection status as active or passive.
- `neighbor – connect-retrycount` - Sets the retry count for the BGP peer.
- `neighbor – local-as` - Updates the local AS used for the peer connection.

redistribute ospf

Command Objective   This command configures the OSPF protocol from which the routes are redistributed into BGP.

The no form of the command disables the redistribution of routes from the given OSPF protocol into BGP. The route map is disassociated from the redistribution, if the no form of the command specifies the route map.

Syntax **redistribute ospf [match {external | internal | nssa-external}] [route-map <string>] [metric <integer>]**

no redistribute ospf [match {external | internal | nssa-external}] [route-map <string>] [metric <integer>]

Parameter Description

- `match {external | internal | nssa-external}` - Matches the OSPF route type to be redistributed into BGP, this object is used only during ospf redistribution. The list contains;
  - external - Redistributes OSPF external routes.
  - internal - Redistributes OSPF internal routes.
  - nssa-external - Redistributes OSPF NSSA external routes.
- `route-map <string(20)>` - Identifies the specified route-map in the list of route-maps during redistribution of routes to BGP. If this is not specified, all routes are redistributed. This value is a string with the maximum size as 20.
- `metric <integer>` - Specifies the metric value for the protocol srecified. This value ranges between 0 and 4294967295. If the metric value not specified, default metric value is considered.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default

- Redistribution is disabled
- Metric - 0
- Redistribution can be configured for only one route map.
- Another route map can be assigned, only if the already assigned route map is disabled.

Example

```
Your Product(config-router)# redistribute ospf match external route-map rm
metric 500
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

neighbor – local-as

Command Objective This command updates the local AS used for the peer connection.

The no form of the command resets the local AS used for the peer connection to the global local-As.

Syntax **neighbor <ip-address|peer-group-name> local-as <AS no>**

no neighbor <ip-address|peer-group-name> local-as

Parameter Description

- `<ip-address>` - Updates the local-as for the IP address of the peer used for the peer connection.
- `<peer-group-name>` - Updates the local-as for the peer group name to which the neighbor is to be added/ removed.
- `local-as <AS no>` - Configures the Autonomous system number for the specified ip address of the peer / peer group name. This value ranges between 1 and 4294967295 or 0.1 to 65535.65535.

  Notes:

  - When four-byte-asn is enabled, this value ranges between 0 and 4294967295or between 0.0 and 65535.65535
  - When four-byte-asn is disabled, this value ranges between 0 and 65535. or between 0.0 and 0.65535
  - When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.0 to 65535.65535

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Auto stop option is disbaled.

Note: This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 10.3.4.5 local-as 1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.
- `show ip bgp peer-group` - Displays information about the peer group.
- `ip bgp four-byte-asn` - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system.
- `bgp asnotation dot` - Changes the output format of BGP ASNs from asplain to asdot notation.

maximum-paths

Command Objective This command sets the BGP multipath count. This is the maximum number BGP multipath routes to be added per destination network in the routing table.

Note: This configuration is effective only after hard/soft reset

The no form of the command resets the bgp multipath count to its default value.

Note: If the no command is executed without the parameter ibgp/eibgp , the maximum path count is set to the default value 1 only for ebgp.

Syntax **maximum-paths [{ibgp |eibgp}] <maximum path>**

no maximum-paths [{ibgp |eibgp}]

Parameter Description

- ibgp - Sets the maximum number of internal bgp multipath routes to be added per destination network in the routing table.
- eibgp - Sets the maximum number of external plus internal BGP multipath routes (with same AS PATH) to be added per destination network in Routing table.
- <maximum path> - Configures the maximum path count for the specified ibgp/ eibgp. This value ranges between 1 and 64.

  Notes:

  - If this is set to 1, only the best route is added to the forwarding table.
  - If the command is executed without the parameter ibgp/eibgp, the maximum path count is configured for ebgp.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 1

Example

```
Your Product(config-router)# maximum-paths eibgp 1
Your Product(config-router-af4)# maximum-paths ibgp 1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp info` – Displays the general information about BGP protocol.

tcp-ao mkt key-id - receive-key-id

Command Objective This command creates a TCP-AO Master Key Tuple (MKT) in the BGP instance.

The no form of the command deletes a TCP-AO MKT in the BGP instance.

Syntax **tcp-ao mkt key-id <Key Id(0-255)> receive-key-id <Rcv Key Id (0-255)> algorithm {hmac-**

sha-1 | aes-128-cmac} key <master-key> [tcp-option-exclude]

no tcp-ao mkt key-id <Key Id(0-255)>

Parameter Description

- `key-id <Key Id(0-255)>` - Configures the send KeyID of the MKT. This value is used to fill the key-id field in the TCP-AO option in the TCP header. This value ranges between 0 and 255.
- `receive-key-id <Rcv Key Id (0-255)>` - Configures the Receive Key-id of the MKT. The MKT ready at the sender to be used for authenticating received segments is indicated to the peer by filling the receive key id of the MKT in of the TCP-AO option in TCP header. This value ranges between 0 and 255.
- `algorithm {hmac-sha-1 | aes-128-cmac}` - Configures the algorithm used for TCP-AO MAC or KDF calculation.
    - `hmac-sha-1` - Sets the algorithm type as hmac-sha-1.
    - `aes-128-cmac` - Sets the algorithm type as aes-128-cmac.

  Note: This algorithm type is currently not supported

- `key <master-key>` - Configures the master key corresponding to the MKT. This value is an octet string with the size between 1 and 80.
- `tcp-option-exclude` - Sets the exclude TCP optionwhich excludes the TCP options other than TCP-AO during MAC calculation, If this is not set TCP-AO MAC will be calculated on TCP segment including all other TCP options.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default algorithm - hmac-sha-1

Note: This command executes only if BGP Speaker Local AS number is configured.

Example

```
Your Product(config-router)# tcp-ao mkt key-id 1 receive- key-id 1
algorithm  hmac-sha-1 key key1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - tcp-ao` - sets BGP peer TCP-AO configurations.
- `neighbor - tcp-ao mkt` - Associates a TCP-AO MKT to the BGP peer.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp - tcp-ao mkt summary` - Displays the BGPrelated TCP-AO MKT information

neighbor - tcp-ao

Command Objective This command sets TCP-AO configurations for the specified BGP Peer.

The no form of the command deletes TCP-AO configurations for the specified BGP peer

Syntax **neighbor <ip-address> tcp-ao { icmp-accept | no-mkt-match packet-discard}**

no neighbor <ip-address> tcp-ao { icmp-accept | no-mkt-match packet-discard}

Parameter Description

- `<ip-address>` - Configures the BGP peer for which the TCP-AO configurations are done.
- `icmp-accept` -. Accepts ICMPv4 type 3 & ICMPv6 type 1 messages for the TCP-AO authenticated peer.
- `no-mkt-match packet-discard` - Discards packet for the peer, if packets are received with TCP-AO and no matching MKT is found.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Auto stop option is disbaled.

Note: This command executes only if BGP Speaker Local AS number and peer is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 tcp-ao icmp-accept
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `tcp-ao mkt key-id - receive-key-id` - Creates a TCP-AO MKT in the BGP instance.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp - tcp-ao neighbor` - Displays the TCP-AO information for the specified BGP peer.

neighbor - tcp-ao mkt

Command Objective This command associates a TCP-AO MKT to the BGP peer.

The no form of the command dissociates a TCP-AO MKT to the BGP peer.

Syntax **neighbor <ip-address> tcp-ao mkt <Key Id(0-255)>**

no neighbor <ip-address> tcp-ao mkt <Key Id(0-255)>

Parameter Description

- `<ip-address>` - Configures the BGP peer for which the TCP-AO MKT configurations are done.
- `<Key Id(0-255)>` -. Configures the Key ID of the MKT which needs to be associated with the peer.. This value ranges between 0 and 255.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Note: This command executes only if BGP Speaker Local AS number and peer is configured.

Example `Your Product(config-router)# neighbor 20.45.0.1 tcp-ao mkt 2`

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `tcp-ao mkt key-id - receive-key-id` - Creates a TCP-AO MKT in the BGP instance.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp - tcp-ao neighbor` - Displays the BGP(v4) neighbor tcp-ao related information.
- `show ip bgp - tcp-ao mkt summary` - Displays the BGPrelated TCP-AO MKT information.

neighbor - tcp-ao mkt - start-accept

Command Objective This command configures the time the router will start accepting packets that have been created with the MKT specified by the key-id.

Note: This command is currently not supported.

Syntax **neighbor <ip-address> tcp-ao mkt <Key Id(0-255)> start-accept <DD-MON-YEAR,HH:MM>**

Parameter Description

- `<ip-address>` - Configures the BGP peer for which the TCP-AO MKT configurations are done.
- `<Key Id(0-255)>` -. Configures the Key ID of the MKT which needs to be associated with the peer. This value ranges between 0 and 255.
- `<DD-MON-YEAR,HH:MM>` - Configures the date and time the router will start accepting packets that have been created with the MKT specified by the key-id. For the router to start accepting packets by 10am on 10 January 2012 the input is given as 10-Jan-2012,10:00

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 0000000000000000

Note: This command executes only if BGP Speaker Local AS number and peer is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 tcp-ao mkt 2 start-accept
10-Jun-2013,10:00
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `show ip bgp peer-group` - Displays information about the peer group.
- `address-family` – Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

neighbor - tcp-ao mkt - stop-accept

Command Objective This command configures the time the router will stop accepting packets that have been created with the MKT specified by the key-id..

Note: This command is currently not supported.

Syntax **neighbor <ip-address> tcp-ao mkt <Key Id(0-255)> stop-accept <DD-MON-YEAR,HH:MM>**

Parameter Description

- `<ip-address>` - Configures the BGP peer for which the TCP-AO MKT configurations are done.
- `<Key Id(0-255)>` -. Configures the Key ID of the MKT which needs to be associated with the peer. This value ranges between 0 and 255.
- `<DD-MON-YEAR,HH:MM>` - The date & time the router will stop accepting packets that have been created with the MKT specified by the key-id. For the router to stop accepting packets by 10am on 10 January 2012 the input is given as 10-Jan-2012,10:00.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 0000000000000000

Note: This command executes only if BGP Speaker Local AS number and peer is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 tcp-ao mkt 2 start-accept
10-Jun-2013,10:00
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `show ip bgp peer-group` - Displays information about the peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

neighbor - tcp-ao mkt - start-generate

Command Objective This command configures the time the router will start generating packets that have been created with the MKT specified by the key-id.

Note: This command is currently not supported.

Syntax **neighbor <ip-address> tcp-ao mkt <Key Id(0-255)> start-generate <DD-MON-YEAR,HH:MM>**

Parameter Description

- `<ip-address>` - Configures the BGP peer for which the TCP-AO MKT configurations are done.
- `<Key Id(0-255)>` -. Configures the Key ID of the MKT which needs to be associated with the peer. This value ranges between 0 and 255.
- `<DD-MON-YEAR,HH:MM>` - Configures the date and time the router will start using the MKT specified by the key-id for packets generation. For the router to start generating packets by 10am on 10 January 2012 the input is given as 10-Jan-2012,10:00.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 0000000000000000

Note: This command executes only if BGP Speaker Local AS number and peer is configured.

Example

```
our Product(config-router)# neighbor 23.45.0.1 tcp-ao mkt 1 start-generate
10-Jan-2012,10:10
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `show ip bgp peer-group` - Displays information about the peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

neighbor - tcp-ao mkt - stop-generate

Command Objective This command configures the time the router will stop generating packets that have been created with the MKT specified by the key-id.

Note: This command is currently not supported.

Syntax **neighbor <ip-address> tcp-ao mkt <Key Id(0-255)> stop-generate <DD-MON-YEAR,HH:MM>**

Parameter Description

- `<ip-address>` - Configures the BGP peer for which the TCP-AO MKT configurations are done.
- `<Key Id(0-255)>` -. Configures the Key ID of the MKT which needs to be associated with the peer. This value ranges between 0 and 255.
- `<DD-MON-YEAR,HH:MM>` - Configures the date and time the router will stop using the MKT specified by the key-id for packets generation. For the router to stop generating packets by 10am on 10 January 2012 the input is given as 10-Jan-2012,10:00.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 0000000000000000

Note: This command executes only if BGP Speaker Local AS number and peer is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 tcp-ao mkt 1 stop-generate
10-Jan-2012,10:10
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `show ip bgp peer-group` - Displays information about the peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

show ip bgp - tcp-ao neighbor

Command Objective This command displays the BGP neighbor tcp-ao related information.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp [vrf <vrf-name>] tcp-ao neighbor [<random_str>]**

Parameter Description

- `vrf <vrf-name>` - Displays BGP neighbor tcp-ao related information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- `<random_str>` - Displays the BGP neighbor tcp-ao configurations for the specified BGP Peer.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp tcp-ao neighbor 23.45.0.1
TCP-AO authentication neighbor summary
---------------------------------------------------------
Context Name : default
-------------------
Neighbor                    : 23.45.0.1
MKT Assigned                : 2
ICMP Processing             : Enabled
No MKT Discard              : Disabled
MKT In-use                  : None
TCP-AO authentication neighbor summary
---------------------------------------------------------
Context Name : vrf1
-------------------
Neighbor                    : 23.45.0.1
TCP-AO is not enabled for this peer!!
```

Related Command(s)

- `neighbor` - tcp-ao - sets BGP peer TCP-AO configurations.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `tcp-ao mkt key-id - receive-key-id` - Creates a TCP-AO MKT in the BGP instance.

show ip bgp - tcp-ao mkt summary

Command Objective This command displays the BGP related TCP-AO MKT information.

Note: The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax **show ip bgp [vrf <vrf-name>] tcp-ao mkt summary**

Parameter Description

- `vrf <vrf-name>` - Displays the BGP related TCP-AO MKT information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp tcp-ao mkt summary
TCP-AO MKT Table
-------------------------
Context Name : default
-------------------
ID(send)    Receive ID   Algorithm  MasterKey       OptionsExclude   Status
---------   ----------   ----------------------     -------------------   ----------
0            1           HMAC-SHA-1  *******    1
Active
255          255         HMAC-SHA-1  *******    1
Active
TCP-AO MKT Table
---------------------------
Context Name : vrf1
-------------------
ID(send)    Receive ID   Algorithm  MasterKey       OptionsExclude   Status
------------   ----------------   --------------   ---------------   ----------------------------   ----------
0            1           HMAC-SHA-1  *******    1
Active
```

Related Command(s)

- `neighbor - tcp-ao mkt` - Associates a TCP-AO MKT to the BGP peer.
- `tcp-ao mkt key-id - receive-key-id` - Creates a TCP-AO MKT in the BGP instance.

ip bgp four-byte-asn

Command Objective This command enables 4-byte ASN support in BGP speaker or in the specified vrf instance created in the system. This value is a string with maximum size as 32.

Note: When VRF is not specified the configurations are done for the default VRF.

The no form of the command disables 4-byte ASN support in BGP or the specified vrf instance created in the system.

Syntax **ip bgp four-byte-asn [vrf <vrf-name>]**

no ip bgp four-byte-asn [vrf <vrf-name>]

Parameter Description

- `vrf <vrf-name>` - Displays the BGP related TCP-AO MKT information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Global Configuration Mode

Default enabled

Note: This command executes only when BGP Speaker Global Admin status is shutdown in the system or the specified vrf insatnce.

Example

```
Your Product(config)# ip bgp four-byte-asn
```

Related Command(s)

- `router-id` - Sets the router ID’s address for the router.
- `bgp router-id` – Configures the BGP Identifier of the BGP Speaker.
- `show ip bgp` – Displays the BGP related information.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

bgp asnotation dot

Command Objective This command changes the output format of BGP ASNs from asplain to asdot notation.

The no form of the command resets the output format of BGP ASNs from asdot to asplain notation.

Syntax **bgp asnotation dot**

no bgp asnotation dot

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default By default, the output format of BGP ASNs is asplain BGP asnotation can be changed only if four-byte-asn is enabled.

Example

```
Your Product(config-router)# bgp asnotation dot
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp info` – Displays the BGP related information.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

33 Loop Protect

The Loop protection provides protection against loops by transmitting Configuration-Test-Protocol packets out of ports on which loop protection has been enabled. When the switch sends out a loop protocol packet and then receives the same packet on a port, it will block the port between transmited port and received port which has disadvantaged

The scope of Loop protect is limited to the configuration of Loop Protection features and related changes on other switch features for supporting Loop Protection.

Spanning-Tree Protocol (STP) in the system plays the similar role with loop protection. Under the physical interface, STP and loop protect should be enabled only one of them.

The list of CLI commands for the configuration of Loop Protect is as follows:

- loop-protect enable
- loop-protect disable
- loop-protect disable-period
- loop-protect transmit-interval
- loop-protect
- show loop-protect

loop-protect enable

Command Objective This command configures the loop-protect enable. The loop-protect enable is a global configuration. By default is diabled. Choose Enable to enable loop protection feature.

Syntax **loop-protect enable**

Parameter Description `enable` - Enable loop protection feature.

Mode Global Configuration Mode

Default disable

Example Your Product(config)# loop-protect enable

Related Command(s)

- `loop-protect disable-period` - loop protection disable period in seconds for ports causing loop ets the IP address for an interface
- `loop-protect transmit-interval` - loop protection transmit interval in seconds
- `loop-protect disable` – Disable loop protection feature
- `show loop-protect` – Dispaly loop protect configuration and status

loop-protect disable

Command Objective This command configures the loop-protect enable. The loop-protect enable is a global configuration. By default is diabled. Choose Enable to enable loop protection feature.

Syntax **loop-protect disable**

Parameter Description `disable` - Enable loop protection feature.

Mode Global Configuration Mode

Default disable

Example

```
Your Product(config)# loop-protect disable
```

Related Command(s)

- `loop-protect disable-period` - loop protection disable period in seconds for ports causing loop ets the IP address for an interface
- `loop-protect transmit-interval` -loop protection transmit interval in seconds
- `loop-protect enable` – Enable loop protection feature
- `show loop-protect` – Dispaly loop protect configuration and status

loop-protect disable-period

Command Objective This command configures the disabled period in seconds for port causing loop. The following Relation should be observed.

Disable Period >= 3*Transmit Interval

The no form of the command configures the loop protect disabled period to its default value.

Syntax **loop-protect disable-period <integer(30-604800)>**

no loop-protect disable-period

Parameter Description `disable-period <integer(30-604800)>` - Configures the parameters for the specified disable period. This value is a string with maximum size as 604800.

Mode Global Configuration Mode

Default Disable-Period - 30 seconds

Example

```
Your Product(config)# loop-protect disable-period 30
```

Related Command(s)

- `loop-protect transmit-interval` - loop protection transmit interval in seconds
- `loop-protect enable` – Enable loop protection feature
- `show loop-protect` – Dispaly loop protect configuration and status

loop-protect transmit-interval

Command Objective This command configures the transmit interval in seconds.

The following Relation should be observed.

Disable Period >= 3*Transmit Interval

The no form of the command configures the loop protect transmit interval to its default value.

Syntax **loop-protect transmit-interval <integer(10-30)>**

no loop-protect transmit-interval

Parameter Description `transmit-interval <integer(10-30)>`- Configures the parameters for the specified transmit inverval. This value is a string with maximum size as 30.

Mode Global Configuration Mode
Default Transmit Inverval - 10 seconds

Example

```
Your Product(config)# loop-protect transmit-interval 10
```

Related Command(s)

- `loop-protect disable-period` - loop protection disable period in seconds for ports causing loop ets the IP address for an interface
- `loop-protect enable` – Enable loop protection feature
- `show loop-protect` – Dispaly loop protect configuration and status

loop-protect

Command Objective This command configure the loop protect test frame format. The number specified by the loop-detection vid command. The switch will send out a loop test frame with specific tag vid. If the command without specific parameter, the switch will send out a un-tag loop test frame.

The no form of the command configures the loop protect test frame. It will remove specific test frame.

Syntax **loop-protect [vid <string>]**

no loop-protect [vid <string>]

Parameter Description `vid <string>`- Configures the parameters for the specified loop protect test frame.

Mode Interface Configuration Mode (Physical Interface Mode)

Default no loop-protect

Example `Your Product(config-if)# loop-protect vid 1-10,20`

Related Command(s)

- `loop-protect disable-period` - loop protection disable period in seconds for ports causing loop ets the IP address for an interface
- `loop-protect transmit-interval` -loop protection transmit interval in seconds
- `loop-protect disable` – Disable loop protection feature
- `show loop-protect` – Dispaly loop protect configuration and status

show loop-protect

Command Objective This command displays loop protect related information available in the switch for the current loop protect enabled in the switch.

The information contain status, transmit interval, disable period and loop-detectd vid.

Syntax **show loop-protect**

Mode Interface Configuration Mode (Physical Interface Mode)

Example

```
Your Product# show loop-protect
Loop Protection       : Disabled
Transmit Interval     : 10 seconds
Disable Period        : 30 seconds
Loop Protection Configured Interfaces
Interface     Status    Loop-Detected( VLAN ID )
--------------  ----------  -------------------------------------------------------
Ex0/1         Up        No
```

Related Command(s)

- `loop-protect disable-period` - loop protection disable period in seconds for ports causing loop ets the IP address for an interface
- `loop-protect transmit-interval` -loop protection transmit interval in seconds
- `loop-protect enable` – Enable loop protection feature
- `loop-protect disable` – Disable loop protection feature

Appendix A Diagnostic Commands

The Diagnostic Commands are simple tools for field debugging, they are not designed for end-users basically, some of the commands may impact the system performance and stability, so please do not use these commands without specialists or technician's instructions.

As the purpose of these commands, some of them can only be used in serial console, if used in telnet or ssh, you will get nothing output from such diagnostic commands. Strongly commended that don't use these command in telnet or ssh sessions.

The list of CLI commands for the diagnostic commands is as follows:

- diag action
- diag bsl-filter
- diag clear counters
- diag pps report
- diag rx dump
- diag show counters
- diag show ets
- diag tsec-filter

diag action

Command Objective This command takes actions of debugging operations or examinations.

This command is only for specialists, end-users should not use this command.

Syntax **diag action <action-name> [<arg1>] [<arg2>] [<arg3>]…**

Mode Privileged EXEC Mode, and Global Configuration Mode

Example

```
No example for specialist command.
```

diag bsl-filter

Command Objective This command switches the BSL status for NP.

This command is only for specialists, and possibly degrade the system performance, end-users should not use this command.

Syntax **diag bsl-filter [{on|off}]**

Mode Privileged EXEC Mode, and Global Configuration Mode

Example

```
No example for specialist command.
APPENDIX A : DIAGNOSTIC COMMANDS
```

diag clear counters

Command Objective This command clears the CPU Rx diagnostic counters, set all counters to zero.

Syntax diag clear counters [force]

Mode Privileged EXEC Mode, and Global Configuration Mode

Example

```
SMIS# diag clear counters
Switch to use counter set #1.
```

Related Command(s) `diag show counters` – List the CPU Rx diagnostic counters.

diag pps report

Command Objective This command reports the CPU Rx rate in every 3 seconds, excute this command again to stop the reporting.

This command will degrade the CPU Rx performance, and possibly impact some protocol operations, please do not use this command without specialist or technican instructions.

Syntax **diag pps report [vrf mgmt]**

Mode Privileged EXEC Mode, and Global Configuration Mode

Example

```
SMIS# diag pps report
NP: Rx pps/rate report ON!
cos-16: 0.3 pps.
cos-3: 0.2 pps.
```

```
cos-16: 0.2 pps.
cos-3: 1400.3 pps.
cos-16: 0.6 pps.
cos-3: 997.3 pps.
cos-16: 0.6 pps.
cos-3: 990.0 pps.
cos-3: 1013.3 pps.
cos-16: 0.6 pps.
cos-3: 1000.3 pps.
SMIS# diag pps report
NP: Rx pps/rate report OFF!
SMIS#
```

Related Command(s) `diag rx dump` – Dump the CPU received packets.

diag rx dump

Command Objective This command dumps each packet received by the CPU, execute agina to stop the dumping.

In a busy network, this command may significantly degrade the CPU Rx performance and impact the stability of the system, please do not use this command without specialist or technican instructions.

It’s recommended that use diag pps report command prior to check the CPU Rx load first. If the CPU Rx rate is higher (> 10 pps), don’t use this command to dump packets.

Syntax **diag rx dump [vrf mgmt]**

Mode Privileged EXEC Mode, and Global Configuration Mode

Example

```
SMIS# diag rx dump
NP: Rx packet dump ON!
SMIS#
SMIS# Pkt#:   [#723,854]
RxLoc:  [DMA:1, U:0, LU:0, LP:59, SGP:34217787, DGP:34217728]
Class:  [COSQ:16, RXCOS:0, IPRI:0]
802.1Q: [V:1, PRI:0, TAG:0]
Length: [PKTLN:68, RXLN:68]
Reason: [FP:0, R32:0x00004000, R:Bpdu Protocol !]
Frame:
       0000: 01 80 c2 00 00 0e 0c c4-7a 1a 44 2e 81 00 00 01
       0010: 88 cc 02 07 04 0c c4 7a-1a 43 f3 04 07 01 45 78
       0020: 30 2f 36 30 06 02 00 14-00 00 00 00 00 00 00 00
       0030: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
       0040: 1c ae 57 e9 ee ee ee ee-ee ee ee ee ee ee ee ee
(end)
SMIS# diag rx dump
NP: Rx packet dump OFF!
SMIS#
```

Related Command(s) `diag pps report` – Show the CPU Rx rate.

diag show counters

Command Objective This command shows the CPU Rx diagnostic counters.

Syntax **diag show counters**

Mode Privileged EXEC Mode, and Global Configuration Mode

Example

```
SMIS# diag clear counters
Switch to use counter set #1.
SMIS#
SMIS# diag show counters
SMC Proprietary Counters:
Date/time: 2017-08-29 17:41:11.934384
RxPkt                      :                               2
RxPktUnit(0)               :                               2
RxPktPort(59)              :                               1
RxPktPort(60)              :                               1
RxPktCos(16)               :                               2
CfaNpRxPkt                 :                               2
CfaNpStkActNotify          :                               2
NpUsrCbCruRxPkt            :                               2
CfaGddRxPkt                :                               2
CfaGddHlHandled            :                               2
CfaIwfRxPkt                :                               2
CfaIwfEnetV2               :                               2
CfaIwfRxUnknown            :                               2
  Current set: 1
  Set size:    2704 bytes
  Total size:  5408 bytes
```

Related Command(s) `diag clear counters` – Clear the CPU Rx diagnostic counters.

diag show ets

Command Objective This command is used to check hardware egress hierarchy status.

Syntax **diag show ets <iftype> <ifnum>**

Mode Privileged EXEC Mode, and Global Configuration Mode

Example No example for specialist command.

diag tsec-filter

Command Objective This command is used to check and set the TSEC filter.

This command is only for specialists. End-users should not use this command.

Syntax **diag tsec-filter [{on|off}]**

Mode Privileged EXEC Mode, and Global Configuration Mode

Example No example for specialist command.

Contacting Supermicro

Headquarters
Address: Super Micro Computer, Inc.
980 Rock Ave.
San Jose, CA 95131 U.S.A.
Tel: +1 (408) 503-8000
Fax: +1 (408) 503-8008
Email: marketing@supermicro.com (General Information)
support@supermicro.com (Technical Support)
Web Site: www.supermicro.com

Europe
Address: Super Micro Computer B.V.
Het Sterrenbeeld 28, 5215 ML
's-Hertogenbosch, The Netherlands
Tel: +31 (0) 73-6400390
Fax: +31 (0) 73-6416525
Email: sales@supermicro.nl (General Information)
support@supermicro.nl (Technical Support)
rma@supermicro.nl (Customer Support)
Web Site: www.supermicro.com.nl

Asia-Pacific
Address: Super Micro Computer, Inc.
3F, No. 150, Jian 1st Rd.
Zhonghe Dist., New Taipei City 235
Taiwan (R.O.C)
Tel: +886-(2) 8226-3990
Fax: +886-(2) 8226-3992
Email: support@supermicro.com.tw
Web Site: www.supermicro.com.tw