Supermicro Switch Configuration

CLI User's Guide

Volume 2

Revision 2.0

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 2.0.0
Release Date: 1/23/2020

Contents

19 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

19.1 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.

☞

- 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.

19.2 vlan

Command Objective

This command creates a VLAN / VFI ID and enters into the config-VLANmode 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 for:

☞

- 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.

19.3 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
```

19.4 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)

☞ 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.

19.5 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.

☞ 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.

19.6 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.

☞ 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.

19.7 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.

☞ 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 shutdown in the switch.

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

19.8 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

☞ 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.

19.9 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

☞ 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.

19.10 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

☞

- 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.

19.11 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

☞

- 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.

19.12 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.

  ✎ 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 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.

    ✐ 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.

    ✐ 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

☞

- 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.

19.13 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.

✎ This command is a complete standardized implementation of the existing command and operates similar to that of the command mac-address-table static multicast. 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

☞

- 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.

19.14 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.
  - deleteOnReset - 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

☞

- 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.

19.15 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

☞

- 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.

19.16 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.

  ✎ 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

☞ 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.

19.17 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.

  ✎ 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

☞

- 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.

19.18 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.

☞

- 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.

19.19 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.

✎ 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.

✎ 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

☞

- 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.

19.20 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.

  ✎ 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.

✎ 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.

✎ The ports configured should be a subset of the member ports.

✎ The ports that are attached to VLAN-aware devices should always be set as untagged ports only.

✎ 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 drop 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

    ✎ 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.

19.21 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.

☞ 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.

19.22 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

☞

- 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.

19.23 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.

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

☞ 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.

19.24 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

☞

- 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.

19.25 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.

✎ 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)

☞

- 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.

19.26 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.

✐ 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)

☞

- 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

19.27 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

☞

- 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.

19.28 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.

☞

- 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.

19.29 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.

☞

- 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.

19.30 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.

✎ 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)

☞

- 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.

19.31 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

☞

- 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.

19.32 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. 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

☞

- 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.

19.33 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

☞ 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.

19.34 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

☞

- 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.

19.35 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

☞

- 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.

19.36 switchport filtering-utility-criteria

Command Objective

This command creates filtering utility criteria for the port. This utility's criteria are 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

☞

- 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

19.37 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.

☞

- 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.

19.38 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.

☞ 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.

19.39 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, Gi0/24
                   Gi0/19, Gi0/20, Gi0/21, Gi0/22,
                   Gi0/23,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.

19.40 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

19.41 show vlan device capabilities

Command Objective

This command displays only the list of VLAN features such as traffic class feature, 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 Commands

- **no shutdown vlan** - Starts and enables VLAN switching feature in the switch.

19.42 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
Gi0/1     0              2
Gi0/1     1              0
Gi0/1     2              1
Gi0/1     3              3
Gi0/      5             5
Gi0/      6             6
Gi0/      7             7
Gi0/      0             2
Gi0/      1             0
Gi0/      2             1
Gi0/      3             3
Gi0/      4             4
Gi0/      5             5
Gi0/      6             6
Gi0/      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.

19.43 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                   :
 00:00:00:00:00:00

 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

 --------------------------------------------------
----- 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.

19.44 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 contains 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.

19.45 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.

19.46 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.

19.47 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.

19.48 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.

19.49 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.

19.50 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   Mac Address        Type     ConnectionId

----   -----------        ----     -----------       ---
--
1      00:10:00:00:00:0   Learnt
       7
2      00:10:00:01:02:0   Learnt
       3
Total Mac Addresses displayed: 2
```

Related Command(s)

- **no shutdown vlan** - Starts and enables VLAN switching feature in the switch.

19.51 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.

19.52 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.

19.53 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  Mac Address         RecvPort  Status   ConnectionId  Ports

----  -----------         --------  ------   ------------  -----

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.

19.54 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       Port
-----------      --------   ------       ----
                                         -
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.

19.55 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.

19.56 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   RecvPortType          Ports

-----------   ------  ----          -----

01:00:5E:01:02:03             static     Gi0/2

01:00:5E:01:02:04             static

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.

19.57 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.

19.58 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.

19.59 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.

19.60 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:       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.

19.61 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.

☞

- 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.

19.62 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

☞

- 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.

19.63 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 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 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

☞

- 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.

19.64 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 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

☞

- 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

19.65 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

☞

- 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 and releases all memories used for the GARP module.
- **`shutdown garp`** - Shuts down the GARP module in the switch on all ports
- **`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.

19.66 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 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 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

☞

- 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 in the 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.

19.67 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

☞

- 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.

19.68 vlan restricted

Command Objective This command configures t feature configures the dyna he restricted VLAN registration feature in a port. This mic registration of VLAN.

Syntax `vlan restricted {enable | disable}`

Parameter Description

- **enable** - Enables restricted VLAN registration feature in the port. The dynamic VLAN entry is permitted only for VLAN registration entries that exist.
- **disable** - Disables recreation or modification of retricted VLAN registration feature in the port. The creation or modification VLANs, for which static of a dynamic VLAN entry is permitted for all VLANs.

Mode Interface Configuration Mode (Physical)

Default disable

☞ 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.

19.69 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

☞ 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.

19.70 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.

☞ 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.

19.71 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

☞ 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.

19.72 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

19.73 private-vlan

Command Objective

This command configures the private vlan type for the vlan to provide layer 2 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

☞ 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

---

19.74 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

☞ 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

19.75 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)

☞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

19.76 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

19.77 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.

19.78 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

19.79 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.

19.80 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

☞ This command executes only if the VLAN is set to active or if the member ports are associated with the VLAN.

Default disable

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.

19.81 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-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>` - 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.

  ✎ 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/ 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.

19.82 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.

☞ 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.

19.83 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

19.84 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 upto 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 an 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        GVRP Packets Received:
Join                   0
Join In                0
Leave In               0
Leave All              0
Empty                  0

Total       GVRP           Packets Transmitted: 0
Join             0
Join In                0
Leave In               0
Leave All              0
Leave                  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

20 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
- vrrp –ping-enable

20.1 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.

20.2 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.

    ✎ 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.

- `<interface-type>` - Enables VRRP 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>** - 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.

✎ 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.

20.3 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

☞ 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.

20.4 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.

✎ 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

☞ 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.

20.5 vrrp group shutdown

Command Objective This command shuts down all VRRP groups.

✎ 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

☞ 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 - show vrrp interface** – Displays the VRRP status information
- **vrid** - Displays the VRRP status information

20.6 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

☞ 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** information.
- **interface - vrid** – Displays the VRRP status

20.7 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` - router will delay before issuing an advertisement claiming master ownership. This value ranges between 0 and 30. 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.

☞ 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

20.8 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

☞ 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.

20.9 vrrp - authentication text

Command Objective This command sets the authentication type for the virtual router to simple password.

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

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.

20.10 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>`

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.

✐ 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

☞This command executes only if the associated primary IP addresses for the virtual router is set.

Syntax `no vrrp <vrid(1-255)> timer`

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

20.11 vrrp - timers advertise

Command Objective This command sets the advertisement timer for a virtual router and sends only the master router advertisements.

✎ 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.

  ✎ 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

☞ 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.

20.12 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.

    ✎ 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.

- **<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.

  ✎ 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.
vlan2      2    255      P  Master  local    12.0.0.
```

```
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.
vlan2      2    255      P  Master  local    12.0.0.
```

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.

20.13 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.

    ✎ 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.

- `<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.

  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

```
P indicates configured to preempt Master

Interface Addr  vrID     Priority    P  State       VRouter     Addr

--------------  ----     ---------   --------       -------     ----

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.

20.14 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
```

20.15 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
```

20.16 vrrp – ping-enable

Command Objective

This command enables VRRP Master to respond pings that are sent to the virtual IP address.

The no form of the command disables the ping reply.

Syntax

```
vrrp <vrid(1-255)> ping-enable

no vrrp <vrid(1-255)> ping-enable
```

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.

Mode

VRRP Interface Configuration Mode

Default

Disabled

☞ Reply ICMP request to the virtual IP address only when it is in master state,

Example

```
Your product(config-vrrp-if)# vrrp 3 ping-enable
```

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

21 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

21.1 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

21.2 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.

Default Sending of ICMP Redirect messages is enabled

☞ 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

21.3 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

☞ 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

21.4 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

☞ VRF instance should be created, before executing this command to configure the ICMP mask reply messages for the context.

Default Sending of ICMP Mask Reply messages is enabled

Example

```
Your Product(config)# ip mask-reply
```

Related Command(s)

- **`ip vrf`** - Creates VRF instance
- **`show ip information`** -– Displays IP configuration information

21.5 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

☞ VRF instance should be created, before executing this command to configure the ICMP echo reply messages for the context.

Default Sending of ICMP Echo Reply messages is enabled

Example

```
Your Product(config)# ip echo-reply
```

Related Command(s)

- `ip vrf` - Creates VRF instance
- `show ip information` -– Displays IP configuration information

21.6 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.

✐ 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

☞ 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

21.7 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

21.8 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

21.9 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.

✎ 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

☞ 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

21.10 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

☞ 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

21.11 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

☞

- 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

21.12 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.

☞ This command is currently not supported in the code.

Syntax

```
ip rarp client

no ip rarp client
```

Mode Interface Configuration Mode

Default Enabled

☞ 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.

21.13 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.

21.14 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

21.15 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      Destinatio  TOS   PMT
```

```
---------      ----------  ---   ---
vr1            14.0.0.25   0     900
```

Related Command(s)

- `ip path mtu` - Sets the MTU for usage in PMTU Discovery

21.16 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

21.16.1 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

☞ 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.

21.16.2 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.

✐ 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.

    ✎ The VLAN ID 4095 is reserved and may be used to indicate a wildcard match for the VID in management operations or Filtering 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>** - 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.

✎ 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

☞

- 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.

21.16.3 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

☞ 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

21.16.4 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

☞ 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

21.16.5 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

☞ 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

21.16.6 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

    ✎ 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.

    ✎ 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 >** - 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 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>** - 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.

  Maximum number of PseudoWire interfaces supported in the system is 100.

Mode Global Configuration Mode

- 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

21.16.7 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 is defined.

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 is 32.
- `<value (2-10)>` - Configures the maximum number of ARP request entries.The value ranges between 2 and 10.

Mode Global Configuration Mode

Default 3

☞ 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

21.16.8 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
```

21.16.9 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

21.16.10 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.

21.16.11 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 is 32.
- **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.

    ✎ 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 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.

  ✎ 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  InBcastPkts     0

0          OutDiscards        0  OutMcastPkts    0
           OutFrgCreates

0          OutForwDgrms       0  OutTrnsmits     0
           OutFrgRqds

0          OutOctets          0  OutMcstOctets   0
           OutBcstPkts

0          DiscntTime         0  1000 RefrshRate  0

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
    InMcastPkt

    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,
```

21.16.12 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

☞ 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 aggregrate-route`** - Sets the maximum number of aggregate routes
- **`ip path mtu discover`** - Enables path mtu discover
- **`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

21.16.13 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.

21.16.14 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.

    ✎ 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 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.

  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 vr1

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 summary

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

21.16.15 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

22 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.

22.1 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
- show ip dhcp client client-id

22.1.1 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

22.1.2 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

☞ 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.

22.1.3 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

☞ 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.

22.1.4 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.

22.1.5 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

22.1.6 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

22.1.7 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

22.1.8 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

22.1.9 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 port channel related configuration can be done, but 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.

22.1.10 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

22.1.11 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
DHCP  Client                              Timer Settings

----  ------                              ----- -------

Fast  Access                              Mode  : Enable

Dhcp     Client   Fast                    Access     DiscoverTimeOut : 5

 Dhcp

 Dhcp        Client

 Client      Fast

 Fast        Access

 Access      NullStateTimeOut : 1

Arp Check TimeOut : 1
```

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

22.1.12 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

22.1.13 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

22.2 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

22.2.1 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)

☞ 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.

22.2.2 ip dhcp server

Command Objective This command adds the configured IP address to the IP address list created for the 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.

✎ 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

22.2.3 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.

☞ 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

22.2.4 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

✎ 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.

22.2.5 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

☞ 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 processingrelated 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.

22.2.6 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)

☞ 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.

22.2.7 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.

☞ 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.

22.2.8 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

22.2.9 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

22.2.10 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.

22.3 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

22.3.1 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)

☞ 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.

22.3.2 service dhcp

Command Objective This command enables the DHCP server in the switch and relay agent features on router which assigns unique IP address and other 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.

☞ 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.

22.3.3 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.

22.3.4 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

22.3.5 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

22.3.6 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

22.3.7 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.

22.3.8 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.

22.3.9 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 the DHCP 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.

22.3.10 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

☞ 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.

22.3.11 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

☞ 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

22.3.12 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

☞ 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.

22.3.13 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

☞ 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.

22.3.14 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

☞ 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.

22.3.15 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

☞ 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.

22.3.16 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

☞

- 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.

22.3.17 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

☞ 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.

22.3.18 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)

☞ 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.

22.3.19 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

☞ 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.

22.3.20 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

22.3.21 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

22.3.22 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.

22.3.23 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                         :
20.0.0.0

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.

22.3.24 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

☞ 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 Expir
        Address Type    Address         State   Time
        ------- ----    -------         ------  -----
        12.0.0. Etherne 00:02:02:03:4:01        May
        2       t                   Assigned    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.

22.3.25 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  2
          :
          -------             -------
          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.

23 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

23.1 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.

☞ 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

23.2 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

☞ 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

23.3 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)

23.4 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

23.5 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

23.6 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

23.7 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

23.8 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

☞ 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

23.9 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).

23.10 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

23.11 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

☞ 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

23.12 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.

23.13 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.

23.14 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

☞ 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

23.15 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

☞ 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.

23.16 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

23.17 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

☞

- 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

23.18 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

☞

- 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.

23.19 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

☞ 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

23.20 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

☞ 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.

23.21 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 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, ...>** - 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

☞ 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.

23.22 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 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, ...>` - 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 typeport-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

☞ 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

23.23 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

☞ 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

23.24 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

23.25 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 an 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)

23.26 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

☞ 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.

23.27 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

☞ 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.

23.28 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.

23.29 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 specific VLAN for a given switch or for all switch (if switch is not specified)

23.30 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)

23.31 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.

23.32 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

☞ 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)

23.33 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

☞

- 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.

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.

23.34 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).

23.35 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.

☞

- 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.

23.36 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.

☞

- 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.

23.37 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.

☞

- 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.

23.38 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.

☞ 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).

23.39 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.

23.40 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 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> / <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

☞ 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.

23.41 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 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.
- `<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 Version 1
  - `v2` – IGMP snooping Version 2
  - `v3` – IGMP snooping Version 3

Mode Config-VLAN Mode

Default v3

☞ 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

23.42 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.

    ✎ 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.

23.43 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.

    ✎ 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.

23.44 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>]`

Parameter Description

- **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.

23.45 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.

    ✎ 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.

23.46 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.

    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

23.47 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.

    ✎ 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)

23.48 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.

    ✎ 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      12.0.0.10    227.1.1.1 Gi0/1  Gi0/3  Gi0/
  2      12.0.0.20    227.1.1.1 Gi0/1  Gi0/3  Gi0/
  2      12.0.0.30    227.1.1.1 Gi0/1  Gi0/2  Gi0/
  2      12.0.0.40    227.1.1.1 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

23.49 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.

    ✎ 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     224.1.1.1           Gi0/2, Gi0/3

   1     224.1.2.3           Gi0/1, 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

23.50 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.

    ✎ 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_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 V2 Leave messages received : 0

IGMP Snooping V1/V2 reports transmitted : 0

IGMP Snooping V3 Block messages received : 0

IGMP Snooping V2 leaves transmitted : 0

IGMP Snooping V3 General queries transmitted : 0

IGMP Snooping V3 Group specific queries transmitted : 2

IGMP Snooping V3 Packets dropped : 1

IGMP Snooping V3 reports transmitted : 3
```

Related Command(s)

- **`ip igmp snooping`** - Enables IGMP snooping in the switch/a specific VLAN

23.51 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.

    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.

23.52 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 (if no 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.

    ✎ 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

☞

- IGMP snooping must be enabled in the switch.
- The port leave mode for an interface must be set as exp-hosttrack

Example

```
Your Product# show ip igmp snooping multicast-receivers

Snooping Receiver Information

-----------------------------

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.

23.53 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.

23.54 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     --
             1

         2     --
             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.

23.55 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.

  ✎ 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.

23.56 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).

23.57 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 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.

- <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

24 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

24.1 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

24.2 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

☞ 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

24.3 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

☞ 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

24.4 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

24.5 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.

☞

- 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)

24.6 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: 0
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

25 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

25.1 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
```

25.2 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
```

26 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

26.1 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.

☞

- 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.

26.2 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

☞

- 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.

26.3 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

☞ 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.

26.4 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

☞ 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.

26.5 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

☞ 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.

26.6 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

☞ 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.

26.7 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.

26.8 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.

26.9 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.

  ✎ `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
```

☞ 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.

26.10 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.
```

☞

- 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.

26.11 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
```

☞

- 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.

26.12 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
```

☞

- 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.

26.13 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
```

☞ 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.

26.14 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
```

☞ 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.

26.15 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
```

☞

- 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.

26.16 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
```

☞

- 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.

26.17 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
```

☞ Meter should have been created.

Related Command(s)

- **meter** – Creates a Meter.
- **show meter –** Displays the Meter entry.

26.18 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
```

☞ 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.

26.19 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
```

☞ 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

26.20 set 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`

☞

- 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.

26.21 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
```

26.22 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.

26.23 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
```

☞ 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

26.24 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
```

☞ 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

26.25 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.

26.26 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
```

☞ 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.

26.27 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    :

        VioNClass    : 0

        ConfAct      : Port 1

        ExcAct       :
        Drop. VioAct
        : Drop.
```

☞ If executed without the optional parameter, this command displays all the available Policy Map. information

Related Command(s) `set policy` – Sets CLASS for policy.

26.28 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.

26.29 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
```

☞ If executed without the optional parameter, this command displays all the available Shape Template information

Related Command(s)

- **`shape-template`** – Creates a Shape Template.

26.30 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
```

☞ 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.

26.31 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
```

☞ 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.

26.32 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
```

☞ 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.

26.33 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     Sched      NextQueue   NextSched
Level                 Index      Id
------- ------------- ---------- ----------- ---------
-- ------ --------

Gi0/1        1            1          0          2

1       1
```

☞ 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.

26.34 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
```

☞ 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.

26.35 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

Gi0/22          0

Gi0/23          0

Gi0/24          0
```

☞ 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.

26.36 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
```

☞ 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.

26.37 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
```

☞ 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.

26.38 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
```

26.39 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
```

26.40 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.

26.41 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    MaxRat
                               e

          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

27 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 have 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
- 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

27.1 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 enable 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

☞ 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

27.2 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

☞ 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.

27.3 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

27.4 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

27.5 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.

✎ 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.

27.6 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

☞ 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

27.7 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)> }} [priority <value (1-255)>]
[redirect {interface <ifXtype> <ifnum> } ]
```

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.
- `flow-label` - Flow identifier in IPv6 header.
- `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.
- `redirect` -F Redirect ACL rule needs additional <ifXtype> <ifnum> parameters to define the port to which the packets matching this ACL rule need to be forwad.

  ✎ This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults priority - 1

☞ 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.

27.8 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

☞

- 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

27.9 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)> }} [priority <value (1-255)>]
```

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.
- `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.

✐ This parameter is not supported in some models due to hardware limitations.

Mode ACL Extended Access List Configuration Mode

Defaults priority - 1

☞ 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.

27.10 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.

✎ 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.

27.11 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.

  ✎ 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.

27.12 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 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.

✐ 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

27.13 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)>]
```

ParameterDescription

- 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 established (1), non-established (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.

✎ 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

27.14 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)>
| l <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.

  ✎ 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.

27.15 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.

    ✎ 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

27.16 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.

  ✎ 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

27.17 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.

  ✐ 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

☞ 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.

27.18 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)>]
```

ParameterDescription

- `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.

  ✎ 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

27.19 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.

  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

27.20 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 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.

  ✎ 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.

27.21 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-
255)>] [redirect {interface <ifXtype> <ifnum> } ]
```

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.

  ✎ This parameter is not supported in some models due to hardware limitations.

- `redirect` - Redirect ACL rule needs additional <ifXtype> <ifnum> parameters to define the port to which the packets matching this ACL rule need to be forwad.

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.

27.22 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 (1-255)>]
```

ParameterDescription

- `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.

  ✎ 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

Example

- priority - 1

Related Command(s)

- **`show access-lists`** **–** Displays the access lists configuration.

27.23 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.

  ✎ 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.

27.24 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

☞

- IP access list must have been created
- ACL is not applicable for DLF packet in egress direction of interface due to H/W ASIC limitation!
- One ACL supports only one egress port. It could not be applied to multiple ports in egress direction.
- 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

27.25 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

☞

- MAC access list must have been created.
- ACL is not applicable for DLF packet in egress direction of interface due to H/W ASIC limitation!
- One ACL supports only one egress port. It could not be applied to multiple ports in egress direction.

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

27.26 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

☞ 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

27.27 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

☞ 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

27.28 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.

  ✎ 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

27.29 show access-lists

Command Objective This command displays the access lists configuration.

Syntax `show access-lists [[{ip | mac | user-defined }] <access-list-number (1-65535)> ]`

Parameter Description

- `ip` - IP Access List
- `mac` - MAC Access List
- `user-defined` - User Defined 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           : 255.255.255.255

         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


 User Defined Access List 1
 -----------------------------
  Priority                          : 5
  Packet Type                       : Ethernet
  Destination MAC Address           : 00:9a:78:56:34:12
  Source MAC Address                : 00:12:34:56:78:9a
  In Port List                     : Ex0/1 , Ex0/2 ,
 Ex0/3 , Ex0/4

                                   , Ex0/5 , Ex0/6

  Out Port                         : Ex0/1

  Filter Action                    : Deny

  Status                           : Actived
```

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

27.30 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
```

☞

- 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

27.31 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-value` - 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
```

27.32 User-defined access-list

Command Objective This command creates a user defined access-list (UDF). The no form of the command deletes the user defined access-list. This value ranges between 1 and 50. The access-list requires to be applied to interface again if there is any modification. And one access-list supports only one egress port. It could not be applied to multiple ports in egress direction.

The no form of the command deletes the UDF.

Syntax

```
user-defined access-list <access-list-number (1-50)>

nno user-defined access-list <access-list-number (1-50)>
```

Mode Global Configuration Mode

Example

```
Your Product(config-if)# user-defined access-list 5

YYour Product(config-userdef-acl)#
```

Related Command(s)

- **permit ip** – A Specifies the packet to be forwarded based on the IP address and associated parameters.
- **show access-lists** – Displays the access list statistics

27.33 permit mac/ip/protocol

Command Objective This command allows traffic for a particular packet if the conditions defined in the permit statement are matched.

Syntax

```
permit {mac {any | host <src-mac-address>} [ {any | host
<dest-mac-address>}] | ip {{any | host <src-ip-address> | <src-
ip-address> <mask> } [ { any |host <dest-ip-address> | <dest-
ip-address>  <mask> } ] } | <protocol-type (1-254)> } [priority
<value (1-255)>]
```

Parameter Description

- `mac | ip | <protocol-type (1-254)>` - The filter type. It can also be a protocol number.
- `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.
- `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 for 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 Ip address of the host that the packet is destined for and the network mask to use with the destination IP address
- `<protocol-type (1-255)>` - IP protocol number
- `priority` - The priority of the UDF 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.

Mode User Defined Configuration Mode

Example

```
Your Product(config)# user-defined access-list 5

Your Product(config-userdef-acl)# permit ip host 10.10.10.1

 any priority 20
```

Related Command(s)

- **`user-defined access-list -`** Create the user defined access-list

27.34 deny mac/ip/protocol

Command Objective This command denies traffic for a particular packet if the conditions defined in the statement are matched.

Syntax

```
deny {mac {any | host <src-mac-address>} [{any | host <dest-mac-address>}] | ip {{any | host <src-ip-address> | <src-ip-address> <mask> } [ { any |host <dest-ip-address> | <dest-ip-address> <mask> } ] } | <protocol-type (1-254)> }  [priority <value (1-255)>]
```

Parameter Description

- `mac | ip | <protocol-type (1-254)>` - The filter type. It can also be a protocol number.
- `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.
- `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 for 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 Ip address of the host that the packet is destined for and the network mask to use with the destination IP address
- `<protocol-type (1-255)>` - IP protocol number
- `priority` - The priority of the UDF 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.

Mode User Defined Configuration Mode

Example

```
Your Product(config)# user-defined access-list 48
 Your Product(config-userdef-acl)# deny mac any host
 00:00:00:00:00:01 priority 20
```

Related Command(s)

- **`user-defined access-list`** **-** Create the user defined access-list

27.35 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)>
} ]  [priority <value (1-255)>]
```

Parameter Description

- `udp` - User Datagram 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
  - the Ip address of the host that the packet is from for the network mask to use with the source IP 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.

  Support either source port or destination port only.

- `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
- `priority` - The priority of the UDF 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.

Mode User Defined Configuration Mode

Example

```
Your Product(config)# user-defined access-list 12

 Your Product(config-userdef-acl)# permit udp host 10.10.10.1
 range 100 200 any priority 23
```

Related Command(s)

- **`user-defined access-list`** **-** Create the user defined access-list

27.36 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)> } ]
```

Parameter Description

- `udp` - User Datagram 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
  - the Ip address of the host that the packet is from for the network mask to use with the source IP 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.

  Support either source port or destination port only.

- `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
- `priority` - The priority of the UDF 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.

Mode User Defined Configuration Mode

Example

```
Your Product(config)# user-defined access-list 12

 Your Product(config-userdef-acl)# deny udp any 10.10.0.0
 255.255.0.0 range 300 400 priority 20
```

Related Command(s)

- **`user-defined access-list`** - Create the user defined access-list

27.37 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)>
} ] [priority <value (1-255)>]
```

Parameter Description

- `tcp` - Transmission ControlProtocol.
- `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 for the network mask to use with the source IP 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.

  Support either source port or destination port only.
- `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
- `priority` - The priority of the UDF 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.

Mode User Defined Configuration Mode

Example

```
Your Product(config)# user-defined access-list 12

Your Product(config-userdef-acl)# permit tcp host 10.10.10.1
eq 1233 any priority 20
```

Related Command(s)

- **user-defined access-list -** Create the user defined access-list

27.38 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)>
} ]  [priority <value (1-255)>]
```

Parameter Description

- `tcp` - Transmission ControlProtocol.
- `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 for the network mask to use with the source IP 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.

  Support either source port or destination port only.

- `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
- `priority` - The priority of the UDF 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.

Mode User Defined Configuration Mode

Example

```
Your Product(config)# user-defined access-list 12

 Your Product(config-userdef-acl)# deny tcp any host
 20.20.20.20 gt 1000 priority 2
```

Related Command(s)

- **user-defined access-list** - Create the user defined access-list

27.39 user-defined access-group

Command Objective This command applies a user defined access list (UDF) to an interface. The no form of this command removes the User defined ACLs from the interface.

User defined access list should be created already, before executing this command.

Syntax

```
user-defined access-group <access-list-number (1-65535)>  {in |
out}

no user-defined access-group [<access-list-number (1-65535)>]
{in | out}
```

Parameter Description

- `access-list-number` – UDF identifier
- in - Inbound packets
- `out` - Outbound packets

Limitation 1: UDF is not applicable for DLF packet in egress direction of interface due to H/W ASIC limitation.

Limitation 2: One ACL supports only one egress port. It could not be applied to multiple ports in egress direction.

Mode Interface Configuration Mode

Example

```
Your Product(config)# user-defined access-list 5

Your Product(config-userdef-acl)# permit tcp host 10.10.10.1 eq

1233 any priority 20

Your Product(config-userdef-acl)# exit

Your Product(config)# inter ex 0/5

Your Product(config-if)# user-defined access-group 5 in
```

Related Command(s)

- **user-defined access-list** - Create the user defined access-list

---

28 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

CHAPTER : BCM_DRAFT

28.1 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.

28.2 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.

28.3 cee-map

Command Objective This command is used 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.

28.4 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

☞ 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       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.

28.5 group

Command Objective This command adds descriptions to priority-groups.

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.

28.6 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.

28.7 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.

28.8 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.

28.9 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.

28.10 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.

28.11 dcbx cee

Command Objective

This command starts DCBX on an interface

No form of this command stops DCBX.

☞ 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.

28.12 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.

No form of this command restores the default settings.

☞ 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.

28.13 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.

☞ 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.

29 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

29.1 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

29.2 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.

29.3 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

Mode

- Authentication – null
- hello-interval – 10 seconds
- retransmit-interval – 5 seconds
- transmit-delay – 1 seconds
- dead-interval – 40 seconds

☞ 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

29.4 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

29.5 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

☞

- 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.

29.6 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

☞ 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

29.7 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

☞ 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.

29.8 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.

29.9 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>]
```

✎ 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

  ✎ 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.

  ✎ 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.

  ✎ This parameter is currently not supported in the no form of the command.
- **cost <value>** - Configures the route path cost.

  ✎ This parameter is currently not supported in the no form of the command.

Mode Router Configuration Mode

Default tag - 2

☞ 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

29.10 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

29.11 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

☞

- 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.

29.12 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

29.13 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

29.14 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

29.15 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.
  - `enabled` – Sets P Bit in the generated Type-7 LSA.
  - `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

☞ 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

29.16 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.

29.17 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.

29.18 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

☞ 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

29.19 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

29.20 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.

☞ 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

29.21 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.

29.22 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.

☞ 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

29.23 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

☞ 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

29.24 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.

☞ 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

29.25 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.

☞ 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

29.26 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

☞ 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

29.27 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

☞ 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

29.28 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)

☞ 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.

29.29 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.

☞ 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

29.30 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)

☞ 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

29.31 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

    ✐ 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 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.

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

29.32 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

☞ 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.

29.33 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

  ✎ 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 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.

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

29.34 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.

29.35 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.

29.36 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
```

☞ This command executes only if the OSPF routing process is enabled.

Related Command(s)

- **router ospf** – Enables OSPF routing process.
- **show ip ospf interface** – Displays OSPF interface information.

29.37 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

☞ This command executes only if theOSPF 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.

29.38 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

☞ 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.

29.39 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

☞ This command executes only if the OSPF 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.

29.40 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

☞ This command executes only if the OSPF 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.

29.41 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.

29.42 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.

29.43 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

☞ This command executes only if the OSPF 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.

29.44 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)

☞

- This command executes only if the OSPF 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.

29.45 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

☞ 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.

29.46 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
  - `sm` - 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.

29.47 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-Bit 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

29.48 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

    ✎ 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 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.

  ✎ 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

29.49 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

    ✎ 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 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.
  - x-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.

  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

29.50 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

    ✐ 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 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.

✎ 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

29.51 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

    ✎ 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 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.

✎ 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.

29.52 show ip ospf - virtual-links

Command Objective This command display the 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

29.53 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

29.54 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
```

```
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

29.55 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.

29.56 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

29.57 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.

29.58 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.

29.59 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.

  ✎ 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)

☞ 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

29.60 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.

✎ 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)

☞ 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

29.61 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.

  ✎ 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)

☞ 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

29.62 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.

✎ 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)

☞ 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

29.63 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

29.64 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.

✎ For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30

Mode OSPF Router Configuration Mode

☞ 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

29.65 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.

  ✎ For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30

Mode OSPF Router Configuration Mode

☞ 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

29.66 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.

  ✎ For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30

Mode OSPF Router Configuration Mode

☞ 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

---

29.67 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

✎ For example, Tuesday May 26, 2013 at 1:30 PM should be configured as, 26-May-2013,13:30

Mode OSPF Router Configuration Mode

☞ 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

---

30 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 an 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

30.1 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 | radius-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.
- `radius-client`–Communicate with RADIUS 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

30.2 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 | radius-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"
- `radius-client` –Default context is "mgmt"

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

30.3 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

30.4 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.

30.5 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

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