Supermicro Switch Configuration

CLI User's Guide

Volume 3

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: 06/30/2017

Contents

31 BGP

The BGP (Border Gateway Protocol) is an inter-autonomous system routing protocol. An autonomous system is a network or group of networks under a common administration and with common routing policies. BGP is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems and is used between Internet service providers (ISP). BGP is often the protocol used between gateway hosts on the Internet. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen.

Hosts using BGP communicate using the Transmission Control Protocol (TCP) and send updated router table information only when one host has detected a change. BGP is commonly used within and between Internet Service Providers (ISPs).

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

- router bgp
- ip bgp dampening
- bgp dampening
- ip bgp overlap-policy
- default-information originate
- ip bgp synchronization
- synchronization
- bgp router-id
- bgp default local-preference
- bgp default ipv4-unicast
- neighbor - remote-as
- neighbor - activate
- neighbor - ebgp-multihop
- neighbor - next-hop-self
- neighbor - interval
- neighbor - timers
- neighbor - shutdown
- neighbor - update-source
- neighbor - gateway
- neighbor - network-address
- neighbor - default-originate
- neighbor - send-community
- neighbor - capability
- bgp nonbgproute-advt
- redistribute
- import route
- bgp always-compare-med
- default-metric
- bgp med

- bgp local-preference
- bgp update-filter
- aggreate-address index
- bgp cluster-id
- bgp client-to-client reflection
- neighbor - route-reflector-client
- bgp comm-route
- bgp comm-filter
- bgp comm-policy
- bgp ecomm-route
- bgp ecomm-filter
- bgp ecomm-policy
- bgp confederation identifier
- bgp confederation peers
- bgp bestpath med confed
- neighbor - password
- address-family
- bgp graceful-restart
- bgp update-delay
- restart-support
- restart-reason
- distribute-list route-map
- distance
- clear ip bgp
- do shutdown ip bgp
- debug ip bgp
- show bgp-version
- show ip bgp
- show ip bgp restart mode
- show ip bgp EndOfRIBMarkerStatus
- show ip bgp restartreason
- show ip bgp restartexitreason
- show ip bgp restartsupport
- show ip bgp restartstatus
- show ip bgp extcommunity - routes
- show ip bgp summary
- show ip bgp filters
- show ip bgp aggregate
- show ip bgp med
- show ip bgp dampening
- show ip bgp local-pref
- show ip bgp timers
- show ip bgp info
- show ip bgp rfl info
- show ip bgp confed info
- show ip bgp community

- show ip bgp extcommunity
- neighbor - maximum-prefix
- neighbor - connect-retry-count
- neighbor - allow-autostop
- neighbor - damp-peer-oscillations
- neighbor delay-open
- bgp trap
- neighbor - peer group
- neighbor <ip-address> peer-group
- neighbor - routemap
- neighbor - transport connection-mode
- nexthop processing-interval
- bgp redistribute internal
- show ip bgp peer-group
- redistribute ospf
- neighbor - local-as
- maximum-paths
- tcp-ao mkt key-id – receive-key-id
- neighbor - tcp-ao
- neighbor - tcp-ao
- neighbor - tcp-ao mkt
- neighbor - tcp-ao - start-accept
- neighbor - tcp-ao - stop-accept
- neighbor - tcp-ao - start-generate
- neighbor - tcp-ao - stop-generate
- show ip bgp - tcp-ao neighbor
- show ip bgp - tcp-ao mkt summary
- ip bgp four-byte-asn
- bgp asnotation dot

31.1 router bgp

Command Objective This command configures the AS (Autonomous System) number of the BGP Speaker and enters into BGP router configuration mode. The no form of the command configures the AS number of the BGP Speaker to its default value.

If this value is already configured to a non-zero value, it must be reset to zero (using no form of the command) before reconfiguring.

Syntax

```
router bgp <AS no> [vrf <vrf-name>]

no router bgp [vrf <string (32)>]
```

Parameter Description

- `vrf <vrf-name>` - Configures the AS (Autonomous System) number of the BGP Speaker for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

  When VRF is not specified the configurations are done for the default VRF.

- `<AS no> -` Configures the AS (Autonomous System) number of the BGP Speaker and enters into BGP router configuration mode. The AS number identifies the BGP router to other routers and tags the routing information passed along This command also allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems. This value ranges between 1 and 4294967295 or 0.1 to 65535.65535.

  When four-byte-asn is enabled, this value ranges between 1 and 4294967295or between 0.1 and 65535.65535

  When four-byte-asn is disabled, this value ranges between 1 and 65535. or between 0.1 and 0.65535

  When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.65535

Mode Global Configuration Mode

Default 0

Example

```
Your Product(config)# router bgp 100
```

Related Command(s)

- `as-num` - Sets the autonomous number for the router.

- **ip address** - Sets the IP address for an interface
- **router-id** - Sets the router ID's address for the router
- **ip bgp dampening** – Configures the Dampening Parameters
- **ip bgp overlap-policy** – Configures the Overlap Route policy for the BGP Speaker
- **ip bgp synchronization / synchronization** – Enables synchronization between BGP and IGP
- **bgp router-id** – Configures the BGP Identifier of the BGP Speaker
- **bgp default local-preference** – Configures the Default Local Preference value
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer
- **neighbor - activate** – Enables default capabilities for the peer and restarts the connnection to the peer if capabilities negotiated change
- **neighbor - ebgp-multihop** – Enables BGP to establish connection with external peers
- **neighbor - next-hop-self** – Enables BGP to send itself as the next hop for advertised routes
- **neighbor - interval** – Configures neighbor interval
- **neighbor - timers**– Configures neighbor KeepAlive Time and Hold Time Intervals
- **neighbor - shutdown** – Disables the Peer session
- **neighbor – update-source** - Configures the source-address for routing updates and for TCP connection establishment with a peer
- **neighbor - gateway** - Configures gateway router's address that will be used as nexthop in the routes advertised to the peer
- **neighbor – network-address** - Configures peer's remote IPv6 network address for IPv4 peer and peer's remote IPv4 network address for IPv6 peer
- **neighbor – default - originate** - Enables advertisement of the default route to the peer
- **neighbor – send-community** – Enables advertisement of community attributes to (standard/extended) to peer
- **neighbor - capability** - Enables the specific BGP capability to be advertised and received from the peer
- **neighbor - delay open** - Configures a delay in sending the first OPEN message to the BGP peer for a specific time period.
- **neighbor - damp-peer-oscillations** - Enables the damp peer oscillation option
- **neighbor - maximum prefix** - Configures the maximum number of peers supported by BGP
- **neighbor – allow-autostop** - Enables the auto stop option to stop the BGP peer and BGP connection automatically
- **neighbor – connect-retrycount** - Sets the retry count for the BGP peer

- **neighbor – transport connection-mode** - Configures the BGP Peer Transport Connection status as active or passive.
- **bgp nonbgproute-advt** – Controls the advertisement of Non-BGP routes
- **no ip bgp overlap-policy** – Resets the Overlap route policy to default
- **redistribute** – Configures the protocol from which the routes have to be redistributed into BGP.
- **bgp always-compare-med** – Enables the comparison of med for routes received from different autonomous system.
- **default-metric** – Configures the Default IGP Metric value
- **bgp med** – Configures an entry in MED Table
- **bgp local-preference** – Configures an entry in Local Preference Table
- **bgp update-filter** – Configures an entry in Update Filter Table
- **aggregate-address index** – Configures an entry in Aggregate Table
- **bgp cluster-id** – Configures the Cluster ID for Route Reflector.
- **bgp client-to-client reflection** – Configures the Route Reflector to support route reflection to Client Peers
- **neighbor** - route-reflector-client – Configures the Peer as Client of the Route Reflector
- **bgp comm-route** – Configures an entry in additive or delete community table
- **bgp comm-filter** – Allows/filters the community attribute while receiving or advertising
- **bgp comm-policy** – Configures the community attribute advertisement policy for specific destination
- **bgp ecomm-route** – Configures an entry in additive or delete ext community table
- **bgp ecomm-filter** – Allows/filters the ext community attribute while receiving or advertising
- **bgp ecomm-policy** – Configures the extended community attribute advertisement policy for specific destination
- **bgp confederation identifier** – Specifies the BGP confederation identifie.
- **bgp confederation peers** – Configures the ASs that belongs to the confederation
- **bgp bestpath med confed** – Enables MED comparison among paths learnt from confed peers
- **neighbor - password** – Configures the password for TCP-MD5 authentication with peer.
- **bgp graceful-restart** - Enables the graceful restart capability.
- **bgp update-delay** - Configures the selection deferral time interval
- **restart-support** - Enables the graceful restart support
- **restart-reason** - Configures the reason for BGP graceful restart

- **distribute-list route-map** - Enables route map filtering for inbound or outbound route
- **distance** - Enables the administrative distance of the routing protocol and sets the administrative distance value
- **debug ip bgp** – Configures the Trace levels.
- **bgp trap** – Enables/disables the bgp trap notification
- **show bgp-version** – Displays the BGP Version information
- **show ip bgp** – Displays the BGP related information
- **show ip bgp community - routes**– Displays routes that belong to specified BGP communities
- **show ip bgp extcommunity - routes** – Displays routes that belong to specified BGP extended-communities
- **show ip bgp summary** – Displays the status of all BGP4 connections
- **show ip bgp filters** – Displays the contents of filter table
- **show ip bgp aggregate** – Displays the contents of aggregate table
- **show ip bgp med** – Displays the contents of MED table
- **show ip bgp dampening** – Displays the contents of dampening table
- **show ip bgp local-pref** – Displays the contents of local preference table
- **show ip bgp timers** – Displays the value of BGP timers
- **show ip bgp info** – Displays the general information about BGP protocol
- **show ip bgp rfl info** – Displays information about RFL feature
- **show ip bgp confed info** – Displays information about confederation feature
- **show ip bgp community** – Displays the contents of community tables
- **show ip bgp extcommunity** – Displays the contents of ext-community tables
- **nexthop processing-interval** - configures the interval at which next hops are monitored for reachablity
- **redistribute ospf** - Configures the OSPF protocol from which the routes are redistributed into BGP
- **show ip bgp - tcp-ao mkt summary** - Displays the BGPrelated TCP-AO MKT information
- **tcp-ao mkt key-id - receive-key-id** - Creates a TCP-AO MKT in the BGP instance
- **neighbor – tcp-ao mkt** - Associates a TCP-AO MKT to the BGP peer
- **neighbor – tcp-ao** – sets BGP peer TCP-AO configurations
- **ip bgp four-byte-asn** - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system
- **bgp asnotation dot** - Changes the output format of BGP ASNs from asplain to asdot notation

31.2 ip bgp dampening

Command Objective This command configures the dampening parameters, changes various BGP route dampening factors and also enables bgp dampening in the system or the specified VRF instance when none of the RFD parameters are specified.

The no form of the command disables the dampening feature in the system or in the specified VRF instance. When the RFD parameter options are not specified in the no form of the command it disables the dampening features and does not reset the values related to RFD.But when the RFD parameter options are specified in the no form of the command, the parameters are reset to its default values.

The RFD parameters configured can be viewed using the `show ip bgp dampening` command even when RFD is disabled.

Syntax

```
ip bgp dampening [vrf <vrf-name>] [HalfLife-Time <integer(600-2700)>] [Reuse-Value <integer(100-1999)>] [Suppress-Value <integer(2000-3999)>] [Max-Suppress-Time <integer(1800-10800)>] [-s Decay-Granularity <integer(1-10800)>] [Reuse-Granularity <integer(15-10800)>] [Reuse-Array-Size <integer(256-65535)>]

no ip bgp dampening [vrf <vrf-name>] [HalfLife-Time [Reuse-Value [Suppress-Value [Max-Suppress-Time]]]] [-s Decay-Granularity [Reuse-Granularity [Reuse-Array-Size]]]
```

Parameter Description

- `vrf <vrf-name>` - Configures the dampening parameters for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

  When VRF is not specified the configurations are done for the default.

- `HalfLife-Time<integer(600-2700)>` - Configures the Time (in seconds) after which a penalty is decreased by half after the half-life period. Once a route has been assigned a penalty, the penalty is decreased for every 5 seconds. BGP's route flap damping algorithm calculates penalty for each routes. This penalty increases by a fixed value when a flap occurs, and decreases exponentially when the route is stable. This value ranges between 600 and 2700.
- `Reuse Value integer(100-1999)>` - Configures the reuse value. If the penalty for a flapping route fallsbelow this value, the route is re-used. The unsuppressing of routes occurs at 10-second increments. This value ranges between 100 and 1999.

  Reuse value can be configured only if the HalfLife Time value is set.

- **Suppress Value<integer(2000-3999)>** - Configures the suppress value. The route is suppressed if the penalty associated with the route exceeds this value. This value ranges between 2000 and 3999.

  Suppress value can be configured only if the HalfLife Time and Reuse value are set.

- **Max-Suppress Time<integer(1800-10800)** - Configures the maximum time (in seconds) a route can be suppressed. This value ranges between 1800 and 10800. Max-Suppress Time can be configured only if the HalfLife Time, Reuse Value and Suppress Value are set.
- **-s Decay Granularity<integer(1-10800)>** - Configures the time granularity in seconds used to perform all decay computations. This value ranges between 1 and 10800.
- **Reuse Granularity<integer(15-10800)>** - Configures the time interval between evaluations of the reuse-lists. Each reuse lists corresponds to an additional time increment. This value ranges between 15 and 10800.
- **Reuse Array Size<integer(256-65535)>** - Configures the size of reuse index arrays. This size determines the accuracy with which suppressed routes can be placed within the set of reuse lists when suppressed for a long time. This value ranges between 256 and 65535.

This command executes only if BGP Speaker Local AS number is configured.

Mode Global Configuration Mode

Default

- HalfLife-Time - 900 seconds
- Reuse Value - 750
- Suppress Value - 2000
- Max-Suppress Time - 3600 seconds
- Decay Granularity - 1 second
- Reuse Granularity - 15
- Reuse Array Size - 1024

Example

```
Your Product(config)# ip bgp dampening HalfLife-Time 1000
reuse-Value 1998 Suppress-Value 2000 -s Decay-Granularity
1 reuse-Granularity 135 reuse-Array-Size 257
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `bgp dampening` – Sets the BGP dampening parameters.
- `show ip bgp dampening` – Displays the contents of dampening table.

31.3 bgp dampening

Command Objective This command configures the Dampening parameters or changes various BGP route dampening factors and. The arguments *half-life*, *reuse*, *suppress*, and *max-suppress-time* are position-dependent hence, if any of them are used, they must all be specified.

The no form of the command disables the bgp dampening feature and does not reset the other configured RFD parameters.

This command is a complete standardized implementation of the existing command and operates similar to that of the command ip bgp dampening.

The RFD parameters configured can be viewed via "show ip bgp dampening" even when RFD is disabled.

Syntax

```
bgp dampening <HalfLife-Time(600-2700)> <Reuse-Value(100-10800)> <Suppress-Value(2000-3999)> <Max-Suppress-Time(1800-10800)>

no bgp dampening
```

Parameter Description

- `<HalfLife-Time (600-2700)>` - Configures the Time (in seconds) after which a penalty is decreased by half. Once a route has been assigned a penalty, the penalty is decreased for every 5 seconds. BGP's route flap damping algorithm calculates penalty for each routes. This penalty increases by a fixed value when a flap occurs, and decreases exponentially when the route is stable. This value ranges between 600 and 2700.
- `<Reuse Value (100-10800)>` - Configures the reuse value. If the penalty for a flapping route falls below this value, the route is re-used. The unsuppressing of routes occurs at 10-second increments. This value ranges between 100 and 10800.

  Reuse value can be configured only if the HalfLife Time value is set.

- `<Suppress Value (2000-3999)>` - Configures the suppress value. The route is suppressed if the penalty associated with the route exceeds this value. This value ranges between 2000 and 3999.

  Suppress value can be configured only if the HalfLife Time and Reuse value are set.

- `<Max-Suppress Time (1800-10800)>` - Configures the maximum time (in seconds) a route can be suppressed. This value ranges between 1800 and 10800.

Max-Suppress Time can be configured only if the HalfLife Time, Reuse Value and Suppress Value are set.

Mode Global Configuration Mode

Default

- HalfLife-Time - 900 seconds
- Reuse Value - 750
- Suppress Value - 2000
- Max-Suppress Time - 3600 seconds

Example

```
Your Product(config-router)# bgp dampening 1000 300 2000 5000
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `ip bgp dampening` – Sets the BGP dampening parameters
- `show ip bgp dampening` – Displays the contents of dampening table.

31.4 ip bgp overlap-policy

Command Objective This command configures the BGP speaker's policy for handling the overlapping routes.

The no form of the command resets the Overlap route policy to its default value. By default, both less and more specific routes are installed.

Syntax

```
ip bgp overlap-policy [vrf <vrf-name>] {more-specific|less-specific|both}

no ip bgp overlap-policy [vrf <vrf-name>]
```

Parameter Description

- `vrf <vrf-name>` - Configures the BGP speaker's policy for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32
- `more-specific` - Configures the Overlap Policy for BGP speaker as more-specific. This implies that when an overlapping route is received more-specific routes are installed in the RIB tree.
- `less-specific` - Configures the Overlap Policy for BGP speaker as less-specific. This implies that when an overlapping route is received less-specific routes are installed in the RIB tree
- `both` - Configures the Overlap Policy for BGP speaker as both. This implies that when an overlapping route is received both more-specific and less-specific routes are installed in the RIB tree

---

Mode Global Configuration Mode

Default Both

This command executes only if BGP Speaker Local AS number is configured and BGP Administrative status is DOWN

Example

```
Your Product(config)# ip bgp overlap-policy more-specific
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker
- `do shutdown ip bgp` – Sets the BGP Speaker Global Admin status DOWN
- `show ip bgp info` – Displays the general information about BGP protocol

31.5 default-information originate

Command Objective This command enables and controls redistribution of default routes of a protocol or network into the BGP and advertisement of the default route (0.0.0.0/0). The default route advertisement is possible only if the default route is present in the IP FDB or it is received from any peers.

The no form of the command disables redistribution and advertisement of the default route. The default routes are not redistributed into BGP.

Syntax

```
default-information originate [vrf <vrf-name>]

no default-information originate [vrf <vrf-name>]
```

Parameter Description

- `vrf <vrf-name>` - Enables and controls redistribution and advertisement of default routes for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32

Mode Global Configuration Mode

Default Default Information Originate is disabled.

☞ This command executes only if BGP Speaker local AS number is configured.

Example

```
Your Product(config)# default-information originate
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp info` - Displays the general information about BGP protocol.

31.6 ip bgp synchronization

Command Objective

This command enables synchronization between Border Gateway Protocol (BGP) and Interior Gateway Protocol (IGP). BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP.

This command allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems.

The no form of the command disables synchronization between BGP and IGP.

Syntax

```
ip bgp synchronization [vrf <vrf-name>]
no ip bgp synchronization [vrf <vrf-name>]
```

Parameter Description

- `vrf <vrf-name>` - Enables synchronization between BGP and IGP for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Global Configuration Mode

Default Synchronization between BGP and IGP is disabled.

☞ This command executes only if BGP Speaker local AS number is configured.

Example

```
Your Product(config)# ip bgp synchronization
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `synchronization` - Enables synchronization between Border Gateway Protocol (BGP) and Interior Gateway Protocol (IGP)
- `show ip bgp info` - Displays the general information about BGP protocol.

31.7 synchronization

Command Objective

This command enables synchronization between Border Gateway Protocol (BGP) and Interior Gateway Protocol (IGP). BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP. This command allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems. The no form of the command disables synchronization between BGP and IGP.

This command is a complete standardized implementation of the existing command and operates similar to that of the command ip bgp synchronization.

Syntax

```
synchronization

no synchronization
```

Parameter Description

- `vrf <vrf-name>` - Enables synchronization between BGP and IGP for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode

BGP Router Configuration Mode

Default

The synchronization between the BGP and IGP is disabled.

Example

```
Your Product(config-router)# synchronization
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `ip bgp synchronization` - Enables synchronization between Border Gateway Protocol (BGP) and Interior Gateway Protocol (IGP)
- `show ip bgp info` - Displays the general information about BGP protocol.

31.8 bgp router-id

Command Objective

This command configures fixed BGP router identifier for a BGP-speaking router. If loopback interface exists, the router ID is set to the highest address for loopback interface otherwise it is set to the highest ip configured on the ip interfaces. Peering sessions will be reset if the router ID is changed. BGP router id is a unique number associated with the BGP speaker. This router-id is advertised to other peers and identifies the BGP speaker uniquely. Administrator can set the router-id of BGP to any value. If router-id is changed, then all the active peer sessions will go DOWN and will be re-started with the new configured router-id.

The no form of the command resets the BGP Identifier of the BGP Speaker to its default value.

Syntax

```
bgp router-id <bgp router id (ip-address)>
no bgp router-id
```

Mode

BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default

The highest interface address is used as the router id.

Example

```
Your Product(config-router)# bgp router-id 10.0.0.1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp` – Displays the BGP related information
- `show ip bgp summary` – Displays the status of all BGP4 connections.
- `address-family` - Enters the router into the address-family router configuration mode.

31.9 bgp default local-preference

Command Objective

This command configures the default local preference value that is to be sent in updates to internal peers. The preference is sent to all routers and access servers in the local autonomous system. This value ranges between 1 and 2147483647.

The no form of the command resets the default local preference to its default value.

Syntax

```
bgp default local-preference <Local Pref Value>
```

Default

100

Example

```
Your Product(config-router)# bgp default local-preference
150
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp info` – Displays the general information about BGP protoco.
- `address-family` - Enters the router into the address-family router configuration mode

---

31.10 bgp default ipv4-unicast

Command Objective

This command enables default routing to IPv4-unicast. By default, the MP (Multi-Protocol) IPv4 Unicast Address Family Capability is negotiated for a peer, when the peer is created. It will not be negotiated for a peer if the default routing configuration is reset. This command affects the negotiation of the MP IPv4 Unicast Address Family Capability for the peers newly created and will not affect the MP IPV4 Unicast negotiation status of the already existing peer.

The no form of the command disables default routing to IPv4 unicast which implies that if a neighbor is created, then IPv4 unicast capability will not be negotiated unless IPv4 unicast capability is explicitly configured for that neighbor.

Syntax `bgp default ipv4-unicast`

`no bgp default ipv4-unicast`

Default The default routing to IPv4-unicast is enabled.

Example

```
Your Product(config-router)# bgp default ipv4-unicast
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode

---

31.11 neighbor - remote-as

Command Objective This command creates a peer and initiates the connection to the peer and adds an entry to the BGP or multiprotocol BGP neighbor table. This specifies a neighbor with an autonomous system number that identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered as external. By default, neighbors that are defined using this command in router configuration mode exchange only unicast address prefixes.

The administrator can create a peer and set the Peer AS number with this command. The configured Peer AS number is compared with the AS number received in the open message and a peer session is initiated only if both the AS numbers match.

The no form of the command disables the peer session and deletes the peer information.

Syntax

```
neighbor <ip-address / peer-group-name> remote-as
<AS no> [allow-autostart [idlehold-time <integer(1-
65535)>]]

no neighbor <random_str> [remote-as <AS no> [allow-
autostart]]
```

Parameter Description

- `<ip-address> / <random_str>` - Configures the BGP peer's remote IP address.
- `<peer-group-name>` - Configures a BGP peer group by using the *peer-group-name* argument. The members of the peer group will inherit the characteristic configured with this command.

  The peer group has be configured prior to setting the remote-as number for the peer-group.

- `remote-as<AS no(1-65535)>` - Configures the Autonomous system number of the peer. This value ranges between 1 and 4294967295 or 0.1 to 65535.65535.

  When four-byte-asn is enabled, this value ranges between 1 and 4294967295 or between 0.1 and 65535.65535

  When four-byte-asn is disabled, this value ranges between 1 and 65535. or between 0.1 and 0.65535

  When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.65535.

- allow-autostart - Starts BGP session with the associated peer automatically. The peer session is automatically started in the IDLE state, after a BGP Peer session is brought down either by Autostop or through reception of invalid BGP message. The BGP session is automatically started after an interval specified by idle hold timer.
- **idlehold-time <integer(1-65535)>** - Configures the idle hold time. This specifies the length of time the BGP peer is held in the Idle state prior to the next automatic restart. This value ranges between 1 and 65535.

 The IdleHoldTime can be configured only when the allow-autostart is enabled

 After each dampening, the value of the Idle Hold Time is doubled consecutively

---

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Example

```
Your Product(config-router)# neighbor 23.45.0.1 remote-as
66
```

Default

- allow-autostart is disabled
- idlehold-time-60 seconds

Related Command(s)

- **router bgp** – Sets the AS number of the BGP Speaker.
- **neighbor - activate** – Enables default capabilities for the peer and restarts the connnection to the peer if capabilities negotiated change
- **neighbor - peer-group** – Creates a peer group.
- **neighbor - ebgp-multihop** – Enables BGP to establish connection with external peers
- **neighbor - next-hop-self** – Enables BGP to send itself as the next hop for advertised routes.
- **neighbor - interval** – Configures neighbor interval
- **neighbor - timers**– Configures neighbor KeepAlive Time and Hold Time Intervals.
- **neighbor - shutdown** – Disables the Peer session
- **neighbor - update-source** - Configures the source-address for routing updates and for TCP connection establishment with a peer.
- **neighbor – gateway** - Configures gateway router's address that will be used as nexthop in the routes advertised to the peer.

- **neighbor - network-address** - Configures peer's remote IPv6 network address for IPv4 peer and peer's remote IPv4 network address for IPv6 peer.
- **neighbor - default-originate** - Enables advertisement of the default route to the peer.
- **neighbor - send-community** – Enables advertisement of community attributes to (standard/extended) to peer.
- **neighbor - capability** - Enables the specific BGP capability to be advertised and received from the peer.
- **neighbor - password** – Configures the password for TCP-MD5 authentication with peer.
- **neighbor delay open** –Configures a delay in sending the first OPEN message to the BGP peer for a specific time period.
- **neighbor damp-peer-oscillations** - Enables the damp peer oscillation option.
- **neighbor maximum prefix** - Configures the maximum number of peers supported by BGP
- **neighbor - allow-autostop** - Enables the auto stop option to stop the BGP peer and BGP connection automatically.
- **neighbor - transport connection-mode** - Configures the BGP Peer Transport Connection status as active or passive
- **neighbor <ip-address> peer-group** – Adds the neighbor as a member of the specified peer group.
- **neighbor** – connect-retrycount - Sets the retry count for the BGP peer
- **show ip bgp summary** - Displays the status of all BGP4 connections.
- **show ip bgp** - Displays the BGP related information.
- **show ip bgp restart mode** - Displays the restart mode of the BGP router and neighbors.
- **show ip bgp EndOfRIBMarkerStatus** - Displays the End_Of_RIB marker status of the BGP router and neighbors.
- **show ip bgp restartexitreason** - Displays the restart exit reason of the BGP.
- **show ip bgp restartsupport** - Displays the restart support of the BGP.
- **show ip bgp restartstatus** –Displays the restart status of the BGP.
- **show ip bgp timers** - Displays the value of BGP timers.
- **show ip bgp info** – Displays the general information about BGP protocol.
- **show ip bgp peer-group** – Displays information abouty the peer group.
- **address-family** - Enters the router into the address-family router configuration mode.
- **neighbot - tcp-ao** - Sets BGP peer TCP-AO configurations.
- **neighbot - tcp-ao mkt** –Associates a TCP-AO MKT to the BGP peer.
- **neighbor tcp-ao mkt - start-accept** - Configures the start accept value for the MKT for the specified BGP peer.
- **neighbor tcp-ao mkt - stop-accept** - Configures the stop accept value for the MKT for the specified BGP peer.

- **neighbor tcp-ao mkt - start-generate** - Configures the start generate value for the MKT for the specified BGP peer.
- **neighbor tcp-ao mkt - stop-generate** - Configures the stop generate value for the MKT for the specified BGP peer.
- **ip bgp four-byte-asn** - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system.
- **bgp asnotation dot** - Changes the output format of BGP ASNs from asplain to asdot notation
- **show ip bgp - tcp-ao neighbor** - Displays the TCP-AO information for the specified BGP peer.

31.12 neighbor - activate

Command Objective This command enables the default capabilities associated with the address-family of the peer. If the capabilities negotiated with the peer are modified due to enabling of the default capabilities, the connection with the peer will be restarted. The default local capabilities for IPv4 peer are “IPv4 Unicast” and “route Refresh”. The default local capabilities for IPv6 peer are “IPv6 Unicast” and “Route Refresh”.

The no form of the command resets the peer after disabling the default capabilities associated with the address-family of the peer.

Syntax

```
neighbor <ip-address|peer-group-name> activate
no neighbor <ip-address> activate
```

Parameter Description

- `<ip-address>` - Enables default capabilities for the specified BGP peer's IP address.
- `<peer-group-name>` - Enables default capabilities for the specified BGP peer group.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 activate
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `show ip bgp` – Displays the BGP related information.
- `show ip bgp info` – Displays the general information about BGP protocol.
- `show ip bgp peer-group` – Displays information abouty the peer group.
- `address-family` - Enters the router into the address-family router configuration mode.

31.13 neighbor – ebgp-multihop

Command Objective This command enables BGP to establish connection with external peers residing on networks that are not directly connected.

By default, external BGP peers need to be directly connected. If external BGP peer are not connected directly, then ebgp-multihop is enabled to initiate the connection with that external peer. If ebgp-multihop is disabled and external BGP peers are indirectly connected, then BGP peer session will not be established.

The no form of the command disables the peer EBGP-Multihop feature.

Syntax

```
neighbor <ip-address | peer-group-name> ebgp-multihop
ebgp-multihop [ttl]

no neighbor <ip-address | peer-group-name> ebgp-
multihop
```

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP-speaking neighbor.
- `<peer-group-name>` - Configures a BGP peer group by using the *peer- group-name* argument. The members of the peer group will inherit the characteristic configured with this command.
- `ttl` - Configures the maximum hop limit that is allowed for indirect BGP session. This value ranges between 1 and 255.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default

- EBGP Multihop is disabled.
- ttl-1

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 ebgp
multihop ttl 20
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `show ip bgp info` – Displays the general information about BGP protocol.
- `show ip bgp peer-group` – Displays information abouty the peer group.
- `address-family` - Enters the router into the address-family router configuration mode.

31.14 neighbor – next-hop-self

Command Objective This command configures the router as the next hop for BGP-speaking neighbor or peer group and enables BGP to send itself as the next hop for advertised routes. Administrator uses this command to make BGP speaker fill its address when advertising routes to the BGP peer. This command is useful in non-meshed networks where BGP neighbors may not have direct access to all other neighbors on the same IP subnet.

The no form of the command resets the peer nexthop-self status to default. The next hop will be generated based on the IP address of the destination and the present next hop in the route information.

Syntax

```
neighbor <ip-address | peer-group-name> next-hop-self

no neighbor <ip-address | peer-group-name> next-hop-self
```

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<peer-group-name>` - Configures a BGP peer group by using the *peer- group-name* argument. The members of the peer group will inherit the characteristic configured with this command.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 next-hop-self
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `show ip bgp info` – Displays the general information about BGP protocol.
- `show ip bgp peer-group` – Displays information abouty the peer group.
- `address-family` - Enters the router into the address-family router configuration mode.

31.15 neighbor – interval

Command Objective This command configures the minimum neighbor interval between the sending of BGP routing updates.

The no form of the command configures the neighbor interval to its default value.

Syntax

```
neighbor <ip-address | peer-group-name> {advertisement-interval <seconds(1-65535)> | as-origination-interval <seconds(1-65535)> | connect-retry-interval <seconds(1-65535)>}

no neighbor <ip-address | peer-group-name> {advertisement-interval | as-origination-interval | connect-retry-interval}
```

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<peer-group-name>` - Configures a BGP peer group by using the *peer- group-name* argument. The members of the peer group will inherit the characteristic configured with this command.
- `advertisement-interval<seconds(1-65535)>` - Configures the advertisement interval which is the time-interval (in seconds) for spacing advertisement of successive external route-updates to the same destination. This value ranges between 1 and 65535.
- `as-origination-interval<seconds(1-65535)>` - Configures the AS origination interval which is the time-interval (in seconds) for spacing successive route-updates originating within the same AS. This value ranges between 1 and 65535.
- `connect-retry-interval<seconds(1-65535)>` - Configures the time interval (in seconds) after which a transport connection with peer is re-initiated. This value ranges between 1 and 65535.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default Advertisement-interval - 30 seconds for EBGP Connections, 5 seconds for IBGP

Connections as-origination-interval - 15 seconds

Connect-retry-interval - 30 seconds

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1
advertisement-interval 45
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `show ip bgp` – Displays the BGP related information.
- `show ip bgp timers` – Displays the value of BGP timers.
- `show ip bgp info` – Displays the general information about BGP protocol.
- `address-family` - Enters the router into the address-family router configuration mode.

31.16 neighbor – timers

Command Objective This command configures neighbor KeepAlive Time and Hold Time Intervals and sets the timers for a specific BGP peer or peer group.

The no form of the command configures the neighbor KeepAlive Time and Hold Time Intervals to its default value.

Syntax

```
neighbor <ip-address | peer-group-name> timers {keepalive
< (1-21845) seconds> | holdtime < (3-65535) seconds> |
delayopentime <(0-65535)seconds>}

no neighbor <ip-address | peer-group-name> timers
{keepalive | holdtime| delayopentime}
```

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<peer-group-name>` - Configures a BGP peer group by using the *peer- group-name* argument. The members of the peer group will inherit the characteristic configured with this command.
- `keepalive < (1-21845) seconds>` - Configures the keep alive interval (in seconds) or frequency with with keep alive messages are sent to its peer for the peer session.The keep-alive value must always be less than the configured hold-time value. The value ranges between 1 and 21845.
- `holdtime < (3-65535) seconds>` - Configures thehold-time interval (in seconds) for the peer, which is sent in the OPEN message to the peer. This is the time interval in seconds for the Hold Time configured for BGP speaker with the peer. The system declares a peer dead, after ensuring that keep alive message is not received within this time period from the peer. This value ranges between 3 and 65535 seconds.
- `delayopentime <(0-65535)seconds>` - Configures the delay open time which is the amount of time that the BGP peer should delay in sending the OPEN message to the remote peer. This value ranges between 0 and 65535.

  The value 0 implies that the BGP Peer can send an OPEN message without any delay to its neighbor.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default keepalive - 30 seconds

holdtime - 90 seconds

Delayopentime - 0 seconds

☞	This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 timers keepalive 40
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `show ip bgp` – Displays the BGP related information.
- `show ip bgp timers` – Displays the value of BGP timers.
- `show ip bgp info` – Displays the general information about BGP protocol.
- `address-family` - Enters the router into the address-family router configuration mode.

31.17 neighbor – shutdown

Command Objective This command disables the Peer session and terminates any active session for the specified neighbor or peer group and removes all associated routing information. In the case of a peer group, a large number of peering sessions could be terminated suddenly.

The no form of the command enables the Peer session for the specified neighbor.

Syntax

```
neighbor <ip-address | peer-group-name> shutdown
no neighbor <ip-address | peer-group-name> shutdown
```

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<peer-group-name>` - Configures a BGP peer group by using the *peer- group-name* argument. The members of the peer group will inherit the characteristic configured with this command.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 shutdown
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `show ip bgp` – Displays the BGP related information.
- `show ip bgp peer-group` – Displays information abouty the peer group.
- `address-family` - Enters the router into the address-family router configuration mode.

31.18 neighbor – update-source

Command Objective This command configures the source-address for routing updates and allows BGP sessions to use any operational interface for TCP connection establishment with a peer.

The no form of the command disables configured source-address for routing updates and for TCP connection establishment with a peer.

Syntax

```
neighbor < ip-address > update-source <random_str>
no neighbor < ip-address > update-source <random_str>
```

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<random_str>` - Configures the IP address to be used as source for routing updates and TCP connection establishment. This IP address can be any interface address.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default The source address is set as 0.0.0.0, and the TCP fills the source address of the TCP session.

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 update-source 40.0.0.1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `show ip bgp` – Displays the BGP related information.
- `address-family` - Enters the router into the address-family router configuration mode.

31.19 neighbor – gateway

Command Objective This command configures gateway router's address that will be used as nexthop in the routes advertised to the peer. This ensures that the traffic coming from this peer is routed through the gateway configured.

The no form of the command resets the configured gateway router's address.

Syntax

```
neighbor < ip-address > gateway <random_str>
no neighbor < ip-address > gateway
```

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<random_str>` - Configures the IP address of the gateway to be used as next hop.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 gateway
10.0.0.1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `show ip bgp` – Displays the BGP related information.
- `address-family` - Enters the router into the address-family router configuration mode.

31.20 neighbor – network-address

Command Objective This command configures peer's remote IPv6 network address for IPv4 peer and peer's remote IPv4 network address for IPv6 peer.

The peer's network address carries the IPv6 network address if the peer's remote-address is an IPv4 address. The peer's network address carries the IPv4 network address if the peer's remote-address is an IPv6 address.

The no form of the command resets network-address configured for the peer.

Syntax

```
neighbor < ip-address > network-address <random_str>
no neighbor < ip-address > network-address <random_str>
```

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<random_str>` - Configures the Remote IP address of the peer.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

☞

- This command executes only if Peer/ Peer Groupis created and Peer AS is configured.
- The peer's remote network address can be configured only after configuring the peer's remote address and the corresponding local interface.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 gateway
10.0.0.1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `show ip bgp` – Displays the BGP related information.
- `address-family` - Enters the router into the address-family router configuration mode.

31.21 neighbor – default-originate

Command Objective This command enables advertisement of the default route to the peer or neighbor for use as a default route. This command overrides the global default route configuration and sends a default route to the peer with self next-hop.

The advertisement occurs irrespective of the presence of default route in FDB.This command does not require the presence of 0.0.0.0 in the local router. When used with a route map, the default route 0.0.0.0 is injected if the route map contains a match ip address clause. The route map can contain other match clauses also.

The no form of the command disables advertisement of the default route to the peer.

Syntax

```
neighbor <ip-address|peer-group-name> default-originate
no neighbor <ip-address|peer-group-name> default-originate
```

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<peer-group-name>` - Configures a BGP peer group by using the *peer-group-name* argument. The members of the peer group will inherit the characteristic configured with this command.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default The advertisement of default route to the peer is disabled.

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 default-originate
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `show ip bgp info` - Displays the general information about BGP protocol.

- `address-family` - Enters the router into the address-family router configuration mode.

31.22 neighbor – send-community

Command Objective This command sends community attribute to a BGP neighbor and enables advertisement of community attributes (standard/extended) to peer.

The no form of the command disables advertisement of community attributes (standard/extended) to peer.

Syntax

```
neighbor < ip-address|peer-group-name > send-community
{both | standard | extended}

no neighbor < ip-address|peer-group-name > send-community
{both | standard |extended}
```

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<peer-group-name>` - Configures a BGP peer group by using the *peer-group-name* argument. The members of the peer group will inherit the characteristic configured with this command.
- `send-community` - Sends the Communities to peer.
  - `both` - Sends both standard and extended communities to peer.
  - `standard` - Sends only standard communities to the peer.
  - `extended` - Sends only extended communities to the peer.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default send-community - both

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 send-
community both
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `show ip bgp info` - Displays the general information about BGP protocol.

- `address-family` - Enters the router into the address-family router configuration mode.

31.23 neighbor – capability

Command Objective This command enables the specific BGP capability to be advertised and received from the peer.

The no form of the command disables the capability for the peer.

Syntax

```
neighbor <ip-address|peer-group-name> capability {ipv4-unicast|ipv6-unicast|route-refresh | orf prefix-list {send | receive | both}}

no neighbor <ip-address|peer-group-name> capability {ipv4-unncast|ipv6-unicast|route-refresh | orf prefix-list {send | receive | both}}
```

Parameter Description

- `<ip-address>` - Configures the IP address of the BGP peer.
- `<peer-group-name>` - Configures a BGP peer group by using the *peer-group-name* argument. The members of the peer group will inherit the characteristic configured with this command.
- `ipv4-unicast` - Sets the IPv4 unicast address family capability.
- `ipv6-unicast` - Sets the MP IPv6 unicast address family capability.
- `route-refresh` - Sets the Route refresh capability.
- `orf prefix-list` - Enables address prefix-based Outbound Route Filter (ORF) for the specified BGP peer group.
  - `send` - Enables ORF send capability.
  - `receive` - Enables ORF recieve capability.
  - `both` - Enables both send and receive ORF Capability.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default By default, ipv4-unicast and route-refresh capabilities are enabled for a peer

---

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 capability ipv4-unicast
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.

- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer.
- **neighbor - peer-group** – Creates a peer group.
- **address-family** - Enters the router into the address-family router configuration mode.

31.24 bgp nonbgproute-advt

Command Objective This command configures the peer type to whom non-bgp routes can be propagated and controls the advertisement of Non-BGP routes either to the external peer or both to internal and external peer.

The no form of the command resets the Non BGP routes advertisement policy to its default value. The Administrator can effectively control the advertisement of the route learnt through Redistribution.

Syntax

```
bgp nonbgproute-advt <external|both>

no bgp nonbgproute-advt
```

Parameter Description

- `external` - Indicates that the non-BGP routes can be exported only to to external peers. All types of non-bgp routes can be propagated to external peers.
- `both` - Indicates that the non-BGP routes can be propagated to both internal and external peers.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default both

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# bgp nonbgproute-advt both
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp info` – Displays the general information about BGP protocol.

31.25 redistribute

Command Objective This command controls redistribution of Direct, Static, IGP(OSPF,RIP) routes into BGP and configures the protocol from which the routes have to be redistributed into BGP after applying the specified route map. If this is set to enable, only the routes from the protocols are imported into BGP and BGP routes will not be distributed to IGP. If this is set as disable, then the routes learned from protocols are removed from BGP and no route is either distributed to or imported from IGP.

The no form of the command disables the redistribution of routes from the given protocol into BGP. The route map is disassociated from the redistribution, if the no form of the command specifies the route map.

Syntax

```
redistribute <static|connected|rip|ospf|all> [route-map <string(20)>] [metric <integer>]

no redistribute <static|connected|rip|ospf|all> [route-map <string(20)>] [metric]
```

Parameter Description

- `static` - Redistributes routes, configured statically, in the BGP routing process.
- `connected` - Redistributes directly connected networks routes, in the BGP routing process.
- `rip` - Redistributes routes that are learnt by the RIP process, in the BGP routing process.
- `ospf` - Redistributes routes, that are learnt by the OSPF process, in the BGP routing process.
- `all` - Redistributes routes, that are learnt by the all processes (RIP, OSPF, statically configured and connected routes), in the BGP routing process
- `route-map <string(20)>` - Identifies the specified route-map in the list of route-maps during redistribution of routes to BGP. If this is not specified, all routes are redistributed. This value is a string with the maximum size as 20.
- `metric <integer>` - Specifies the metric value for the routes to redistribute to bgp. This value ranges between 0 and 4294967295. If the metric value not specified, default metric value is considered.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default Redistribution is disabled

☞ Redistribution can be configured for only one route map. Another route map can be assigned, only if the already assigned route map is disabled.

Example

```
Your Product(config-router)# redistribute all route-map rm
metric 500
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.

31.26 import route

Command Objective This command adds non-BGP IP routes imported into the BGP RIB and allows importing a static route into BGP, after updating the RIB tree, if there is any change in the best route selected, then the route is updated to the Common Forwarding table.

Syntax `import route ip-address prefixlen nexthop metric ifindex protocol action route-count`

Parameter Description

- `ip-address` - Configures the Prefix of the route to be imported.
- `prefixlen` - Configures the number of high-order bits in the IP address These bits are common among all hosts within a network. This value ranges between 1 and 32.
- `nexthop` - Configures the Nexthop IP address for the route.
- `metric` - Configures the metric value for the routes being imported. This value ranges between 1 and 2147483647.
- `ifindex -` Configures the interface index of the route. This value ranges between 1 and 2147483647.
- `protocol` - Configures the Protocol value for the non-BGP routes. The values can be:
  - 2 – Local.
  - 3 – Static.
  - 8 – RIP.
  - 13 – OSPF

  Only STATIC routes (protocol 3) can be added through Common Forwarding table. All non-BGP protocol (Local, Static, RIP, OSPF) routes can be viewed.

- `action` - Controls addition or deletion of the non bgp routes. The options are:
  - `Add` – Specifies the addition of non bgp routes.
  - `Delete`- Specifies the deletion of non bgp routes.
- `route-count` - Configures the number of routes to be imported.

Mode BGP Router Configuration Mode

Example

```
Your Product(config-router)# import route 23.45.0.1 10
23.45.0.10 10 2 3 add 4
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.

31.27 bgp always-compare-med

Command Objective This command enables the comparison of Multi Exit Discriminator (MED) for routes received from different autonomous system. The MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED.

The no form of the command disables the comparison of MED for routes received from different autonomous system. MED will be compared only for routes from same neighbor autonomous system.

Syntax

```
bgp always-compare-med

no bgp always-compare-med
```

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default The comparison of MED for routes received from different autonomous system is disabled

---

Example

```
Your Product(config-router)# bgp always-compare-med
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp info` - Displays the general information about BGP protocol.
- `address-family` - Enters the router into the address-family router configuration mode.

31.28 default-metric

Command Objective This command configures the default IGP metric value for routes redistributed into BGP with the redistribute command. A default metric can be configured to solve the problem of redistributing routes with incompatible metrics. Assigning the default metric will allow redistribution to occur. This value ranges between 0 and 2147483647.

The no form of the command resets the Default IGP Metric value to its default value 0. If configured to 0, the metric received from the IGP route will be used. If configured to any other value, the MED value of the redistributed routes take this value. This value has no effect on the Direct routes.

Syntax

```
default-metric <Default Metric Value(0-2147483647)>

no default-metric
```

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default 0

Example

```
Your Product(config-router)# default-metric 300
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp info` - Displays the general information about BGP protocol.
- `address-family` - Enters the router into the address-family router configuration mode.

31.29 bgp med

Command Objective This command configures an entry in BGP4 MED Table and contains the MED values that are to be assigned to routes.

The no form of the command deletes the entry from MED Table or BGP4 MED table. The entry will not be matched when the MED value for an update is calculated, if the prefix length is set as zero.

Syntax

```
bgp med <1-100> remote-as <AS no> <ip-address> <prefixlen>
[intermediate-as <AS-no list- AS1,AS2,...>] value <value>
direction {in|out}[override]

no bgp med <1-100>
```

Parameter Description

- `med <1-100>` - Configures the entry containing information about the MED value. This value ranges between 1 and 100.
- `remote-as < AS no >` - Configures the Autonomous system number that identifies the BGP router to other routers and tags the routing information passed along. This value ranges between 0 and 4294967295 or 0.1 to 65535.65535.

  When four-byte-asn is enabled, this value ranges between 0 and 4294967295or between 0.0 and 65535.65535

  When four-byte-asn is disabled, this value ranges between 0 and 65535. or between 0.0 and 0.65535

  When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.0 to 65535.65535

  A value of zero indicates that this entry is not valid and will not be matched for when the MED value for an update is calculated

- `<ip-address>` - Configures the Route-prefix on which MED policy needs to be applied.
- `<prefixlen>` - Configures the number of high-order bits in the IP address. This is the length of the IP address prefix in the Network Layer Reachability Information (NLRI) field . These bits are common among all hosts within a network. This value ranges between 0 and 32.

  A value of zero indicates that this entry is not valid and will not be matched for when the MED value for an update is calculated.

- **intermediate-as<AS-no list- AS1,AS2,...>** - Configures the sequence of intermediate Autonomous system numbers through which the route update is expected to travel. This is a Comma separated list of AS numbers that are to be checked against the AS_PATH attribute of the updates. This valus is a string with the maximum size as 100.
- **Value <value>** - Configures the value assigned to the MED attribute for the route present in NLRI. This value ranges between 0 .and 2147483647.
- **direction** - Configures the direction of application of MED policy.
  - **in** – Indicates that on received route-update with other matching attributes like as-number, intermediate-as numbers
  - **out** - Indicates that on route-update that needs to be advertised to peer
- **override** - Decides whether the configured MED value will override the received MED value.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default

- remote-as - 0
- Prefixlen - 0
- direction - In
- Value - 0

Example

```
Your Product(config-router)# bgp med 5 remote-as 200
212.23.45.0 24 intermediate-as 150 value 50 direction in
override
```

Related Command(s)

- **router bgp** – Sets the AS number of the BGP Speaker.
- **show ip bgp med** – Displays the contents of MED table
- **address-family** - Enters the router into the address-family router configuration mode.
- **ip bgp four-byte-asn** - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system
- **bgp asnotation dot** - Changes the output format of BGP ASNs from asplain to asdot notation.

31.30 bgp local-preference

Command Objective This command configures an entry in the Local Preference Table. This table contains the value that is to be assigned to the Local Preference attibute.

The no form of the command deletes the entry from Local Preference Table.

Syntax

```
bgp local-preference <1-100> remote-as <AS no> <ip-address> <prefixlen> [intermediate-as <AS-no list-AS1,AS2,...>] value <value> direction {in|out} [override]

no bgp local-preference <1-100>
```

Parameter Description

- `local-preference <1-100>` - Configures the local preference index. This value ranges between 1 and 100.
- `remote-as < AS no >` - Configures the Autonomous system number that identifies the BGP router to other routers and tags the routing information passed along. This value ranges between 0 and 4294967295 or 0.1 to 65535.65535.

  When four-byte-asn is enabled, this value ranges between 0 and 4294967295or between 0.0 and 65535.65535

  When four-byte-asn is disabled, this value ranges between 0 and 65535. or between 0.0 and 0.65535

  When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.0 to 65535.65535

- `<ip-address>` - Configures the route prefix in the Network Layer Reachability Information on which local-preference policy needs to be applied. The input route ip address can be an ipv4 or an ipv6 address.
- `<prefixlen>` - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges between 0 and 32 for ipv4 address and 0 to 128 for ipv6 address.

  A value of zero indicates that this entry is not valid and will not be matched for when the MED value for an update is calculated.

- `intermediate-as<AS-no list- AS1,AS2,...>` - Configures the sequence of intermediate AS numbers through which the route update is expected to travel or a Comma separated list of AS numbers that are to be checked against the AS_PATH attribute of the updates. This value is a list with the maximum size as 100.

- **Value <value>** - Configures the local-preference value that needs to be associated with the route-update. This value ranges between 0 .and 2147483647.
- **direction** - Specifiies the direction of the application of local-preference **in** – Indicates that on received route-update with other matching attributes like as-number, intermediate-as numbers
  - **out** - Indicates that on route-update that needs to be advertised to peer
  - **override** - Decides whether configured local-preference value overrides the received local-preference value. If this keyword is not specified, then the received value will have precedence over configured value.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default

- remote-as - 0
- direction - In
- Value - 100
- ip-address – 0.0.0.0
- Prefixlen - 0

Example

```
Your Product(config-router)# bgp local-preference 5
remote-as 200 21.3.0.0 16 intermediate-as 150 value 250
direction out override
```

Related Command(s)

- **router bgp** – Sets the AS number of the BGP Speaker.
- **show ip bgp local-pref** – Displays the contents of local preference table.
- **address-family** - Enters the router into the address-family router configuration mode.
- **ip bgp four-byte-asn** - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system
- **bgp asnotation dot** - Changes the output format of BGP ASNs from asplain to asdot notation.

31.31 bgp update-filter

Command Objective This command configures an entry in Update Filter Table which contains rules to filter out updates based on the AS from which it is received, Network Layer Reachability Information (NLRI) and AS through which it had passed.

The no form of the command deletes the entry from Update Filter Table.

Syntax

```
bgp update-filter <1-100> {permit|deny} remote-as <AS no>
<ip-address> <prefixlen> [intermediate-as <AS-no list-
AS1,AS2,...>] direction {in|out}

no bgp update-filter <1-100>
```

Parameter Description

- `update-filter <1-100>` - Configures the entry containing information about the updates that are to be filtered. This value ranges between 1 and 100.
- `permit` - Allows the route to pass filter policy test.
- `deny` - Filters the routes when it passes through filter policy test
- `remote-as < AS no >` - Configures the Autonomous system number that identifies the BGP router to other routers and tags the routing information passed along. This value ranges between 0 and 4294967295 or 0.1 to 65535.65535.

  When four-byte-asn is enabled, this value ranges between 0 and 4294967295or between 0.0 and 65535.65535

  When four-byte-asn is disabled, this value ranges between 0 and 65535. or between 0.0 and 0.65535

  When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.0 to 65535.65535

- `<ip-address>` - Configures the route prefix in the Network Layer Reachability Information on which the filter needs to be applied.
- `<prefixlen>` - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges between 0 and 32 for ipv4 address and 0 to 128 for ipv6 address.

  The NLRI field will not be matched if the prefix length is set as zero.

- `intermediate-as<AS-no list- AS1,AS2,...>` - Configures the sequence of intermediate AS numbers through which the route update is expected to travel or a Comma separated list of AS numbers that are to be checked against the AS_PATH attribute of the updates. This value is a list with the maximum size as 100.

- **direction** - Specifiies the direction of the application of filters with which the entry is to be associated
  - **in** – Indicates that on received route-update with other matching attributes like as-number, intermediate-as numbers
  - **out** - Indicates that on route-update that needs to be advertised to peer

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default

- remote-as - 0
- direction - In
- ip-address – 0.0.0.0
- Prefixlen - 0

Example

```
Your Product(config-router)# bgp update-filter 6 deny
remote-as 145 72.93.0.0 14 intermediate-as 150 direction
in
```

Related Command(s)

- **router bgp** – Sets the AS number of the BGP Speaker.
- **show ip bgp filters** – Displays the contents of filter table
- **address-family** - Enters the router into the address-family router configuration mode.
- **ip bgp four-byte-asn** - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system
- **bgp asnotation dot** - Changes the output format of BGP ASNs from asplain to asdot notation.

31.32 aggregate-address index

Command Objective This command creates an aggregate entry in a BGP or multiprotocol BGP routing table if any more-specific BGP or multiprotocol BGP routes are available that fall in the specified range. The entries in the table specifies the IP address based on which the routing information has to be aggregated. The aggregate route will be advertised as coming from autonomous system. The atomic aggregate attribute will be set only if some of the information in the AS PATH is missing in the aggregated route, else it will not be set.

The no form of the command deletes the specified entry from the aggregate table.

Syntax

```
aggregate-address index <1-100> <ip-address> <prefixlen>
[summary-only] [as-set] [suppress-map map-name]
[advertise-map map-name] [attribute-map map-name

no aggregate-address index <1-100>
```

Parameter Description

- `index <1-100>` - Configures the entry containing information about the IP address on which the aggregation has to be done. This value ranges between 1 and 100.
- `<ip-address>` - Configures route prefix in the Network Layer Reachability Information on which aggregate policy needs to be applied
- `<prefixlen>` - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges between 0 and 32 for IPv4 address and between 0 and 128 for IPv6 Address.
- `summary-only` - Specifies that aggregated (summarized) route alone will be sent to the peers.

  If this is not specified, both the summary and the more-specific routes based on which the summary entry was generated are be advertised to the peers.

- `as-set` - Generates autonomous system set path information.
- `suppress-map map-name` - Specifies the name of the route map used to select the routes to be suppressed. The route map contains the rules for suppressing the more-specific routes in forming the aggregate route. When suppress-map configuration is used along with summaryonly option, summary-only configuration command does'nt have any effect. And the more-specific routes that the suppress-map suppresses are not advertised. Other routes are advertised in addition to the aggregated route. This value is a string with a maximum length of 20.

- **advertise-map map-name** - Specifies the name of the route map used to select for forming aggregate routes. The route map contains the rules for selecting specific routes for aggregation Other routes are advertised. When advertise-map is used, only advertise-map influences the creation of aggregate entry. In absence of advertise-map, the aggregate route inherits the attributes of the more specific routes, both suppressed and unsuppressed. This value is a string with a maximum length of 20.
- **attribute-map map-name** - Specifies the name of the route map used to form the attribute of the aggregate route. The route map contains the rules for setting the attributes for the aggregated route. When attribute-map and advertise-map along with autonomous system set path information are enabled and other configurations, the attribute-map overrides the attribute that is formed with the routes selected by the advertise-map. This value is a string with a maximum length of 20.

Mode	BGP Router Configuration Mode / Address Family Router Configuration Mode
☞	The IP address and the prefix length can be configured, only if the Aggregate admin status of the BGP is down.
Example	`Your Product(config-router)# aggregate-address index 1 21.1.0.0 16 summary-only`

Related Command(s)

- **router bgp** – Sets the AS number of the BGP Speaker.
- **show ip bgp aggregate** – Displays the contents of aggregate table
- **address-family** - Enters the router into the address-family router configuration mode.

31.33 bgp cluster-id

Command Objective This command configures the Cluster ID for the Router Reflector of the BGP cluster which has more than one route reflector. This value ranges between 1 and 4294967295.

Usually in a cluster of clients with single route reflector the cluster is identified by the router ID of the route reflector. In order to increase redundancy and avoid a single point of failure, a cluster might have more than one route reflector. In this case, all route reflectors in the cluster must be configured with the 4-byte cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster.

The no form of the command resets the Cluster ID for the Route Reflector.

Syntax

```
bgp cluster-id {cluster id value ip_address/integer}

no bgp cluster-id
```

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Example

```
Your Product(config-router)# bgp cluster-id 10.0.0.1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp rfl info` – Displays information about RFL feature.
- `address-family` - Enters the router into the address-family router configuration mode.

31.34 client-to-client reflection

Command Objective This command configures the Route Reflector to support route reflection to Client Peers. By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. If the clients are fully meshed, route reflection is not required.

The no form of the command disables client-to-client reflection. If disabled, then Route Reflector will not advertise routes learnt from a client peer to other client peers. This occurs when all peers within a cluster are fully-meshed and the client peer itself is able to advertise routes to other clients of the route-reflector.

Syntax

```
bgp client-to-client reflection

no bgp client-to-client reflection
```

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default Route Reflector will reflect routes learnt from a client peer to all other client peers.

Example

```
Your Product(config-router)# bgp client-to-client
reflection
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp rfl info` – Displays information about RFL feature.
- `address-family` - Enters the router into the address-family router configuration mode.

31.35 neighbor - route-reflector-client

Command Objective This command controls client-to-client reflection and configures the specified Peer as Client of the Route Reflector. All the neighbors configured with this command will be members of the client group and the remaining IBGP peers will be members of the nonclient group for the local route reflector.

The no form of the command resets the Peer as conventional BGP Peer.

Syntax

```
neighbor <ip-address | peer-group-name> route-reflector-client

no neighbor <ip-address | peer-group-name> route-reflector-client
```

Parameter Description

- `<ip-address>` - Configures the Peer's Remote IP address of the BGP neighbor being identified as a client.
- `<peer-group-name>` - Configures a BGP peer group by using the *peer-group-name* argument. Tthe members of the peer group will inherit the characteristic configured with this command.

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

Mode BGP Router Configuration Mode/ Address Family Router Configuration Mode

---

This command executes only if Peer is created.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 route-reflector-client
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer
- `address-family` - Enters the router into the address-family router configuration mode
- `show ip bgp rfl info` – Displays information about RFL feature

31.36 bgp comm-route

Command Objective This command configures an entry in additive or delete community table for a given destination.

The no form of the command removes the entry from additive or delete community table.

Syntax

```
bgp comm-route {additive|delete} <ip-address> <prefixlen> comm-value <4294967041-4294967043,65536-4294901759>
```

```
no bgp comm-route {additive|delete} <ip-address> <prefixlen> comm-value <4294967041-4294967043,65536-4294901759>
```

Parameter Description

- `additive` - Adds associated community value with the already existing communities in the route update.
- `delete` - Removes the community attribute from the route-prefix when it passes through the filter process.
- `<ip-address>` - Configures the Route prefix on which community policy needs to be applied.
- `<prefixlen>` - Configures the IP prefix length for the destination. These bits are common among all hosts within a network. This value ranges between 1 and 32.
- `comm-value <4294967041-4294967043,65536-4294901759>` - Configures the Community attribute value. This value ranges between 4294967041 and 4294967043 or between 65536 and 4294901759.

Mode BGP Router Configuration Mode/ Address Family Router Configuration Mode

---

☞ This command executes only if Peer is created.

Example

```
Your Product(config-router)# bgp comm-route additive 24.5.0.0 16 comm-value 429490
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode
- `show ip bgp community`– Displays the contents of route/peer/filter/policy community tables.

31.37 bgp comm-filter

Command Objective This command allows/ filters the community attribute while receiving or advertising. The rules to filter out the updates are based on the AS from which it is received, NLRI and AS through which it had passed.

The no form of the command removes the filter policy for the community attribute.

Syntax

```
bgp comm-filter <comm-value(4294967041-4294967043,65536-4294901759)> <permit|deny> <in|out>

no bgp comm-filter <comm-value(4294967041-4294967043,65536-4294901759)> <permit|deny> <in|out>
```

Parameter Description

- `comm-value(4294967041-4294967043,65536-4294901759)>` - Configures the Community Attribute Value. This value ranges between 4294967041 and 4294967043 or between 65536 and 4294901759.
- `permit` - Allows a particular community attribute to be received or advertised in updates.
- `deny` - Filters the routes containing the community attribute value in received or advertised updates.
- `in` - Configures the direction of route-updates on which the community filter policy needs to be applied as in. This indicates that the community filter needs to be applied on received routes.
- `out` - Configures the direction of route-updates on which the community filter policy needs to be applied as out. This indicates that the community filter needs to be applied on routes advertised to peers.

Mode BGP Router Configuration Mode/ Address Family Router Configuration Mode

---

Default permit

Example

```
Your Product(config-router)# bgp comm-filter 75100 deny in
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode
- `show ip bgp community`– Displays the contents of route/peer/filter/policy community tables.

31.38 bgp comm-policy

Command Objective This command configures the community attribute advertisement policy for specific destination.

The no form of the command removes the community attribute advertisement policy for specific destination.

Syntax

```
bgp comm-policy <ip-address> <prefixlen> <set-add|set-none|modify>

no bgp comm-policy <ip-address> <prefixlen>
```

Parameter Description

- `<ip-address>` - Configures the Route prefix on which community policy needs to be applied.
- `<prefixlen>` - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges between 1 and 32.
- `set-add` - Sends only the configured additive communities with associated route.
- `set-none` - Sends the associated route without any communities.
- `modify` - Removes the associated route with received delete communities and adds the configured additive communities.

Mode BGP Router Configuration Mode/ Address Family Router Configuration Mode

---

Default modify

Example

```
Your Product(config-router)# bgp comm-policy 24.5.0.0 10 set-none
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode
- `show ip bgp community`– Displays the contents of route/peer/filter/policy community tables.

31.39 bgp ecomm-route

Command Objective This command configures an entry in additive or delete extended community table.

The no form of the command removes the entry from additive or delete extended community table.

Syntax

```
bgp ecomm-route {additive|delete} <ip-address> <prefixlen>
ecomm-value <value(xx:xx:xx:xx:xx:xx:xx:xx)>

no bgp ecomm-route {additive|delete} <ip-address>
<prefixlen> ecomm-value <value(xx:xx:xx:xx:xx:xx:xx:xx)>
```

Parameter Description

- `additive` - Adds associated extended-community value with the already existing communities in the route update.
- `delete` - Removes the extended-community attribute from the route-prefix when it passes through the filter process.
- `<ip-address>` - Configures the Route prefix on which community policy needs to be applied.
- `<prefixlen>` - Configures the IP prefix length for the destination. These bits are common among all hosts within a network. This value ranges between 1 and 32.
- `ecomm-value <value(xx:xx:xx:xx:xx:xx:xx:xx)>` - Configures the Extended Community Attribute Value. This is an octet string value.

Mode BGP Router Configuration Mode/ Address Family Router Configuration Mode

---

Example

```
Your Product(config-router)# bgp ecomm-route additive
12.0.0.0 2 ecomm-value 01:01:22:33:44:55:66:77
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode
- `show ip bgp extcommunity` – Displays the contents of route ext-community route tables.

31.40 bgp ecomm-filter

Command Objective This command allows/ filters the extended community attribute while receiving or advertising.

The no form of the command removes the filter policy for the extended community attribute.

Syntax

```
bgp ecomm-filter <ecomm-value(xx:xx:xx:xx:xx:xx:xx:xx)>
{permit|deny} {in|out}

no bgp ecomm-filter <ecomm-value(xx:xx:xx:xx:xx:xx:xx:xx)>
{permit|deny} {in|out}
```

Parameter Description

- `<ecomm-value(xx:xx:xx:xx:xx:xx:xx:xx)>` - Configures the extended community value. This is an octet string value in the form xx:xx:xx:xx:xx:xx:xx:xx.
- `permit` - Allows the route -update with the associated extended community value to pass the filter test.
- `deny` - Denies the route-update with the associated extended community value to pass the filter test.
- `in` - Configures the incoming direction of applied filter.
- `out` - Configures the outgoing direction of applied filter.

Mode BGP Router Configuration Mode/ Address Family Router Configuration Mode

---

Default permit

Example

```
Your Product(config-router)# bgp ecomm-filter
01:01:22:33:23:43:44:22 deny in
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode
- `show ip bgp extcommunity` – Displays the contents of ext-community route table.

31.41 bgp ecomm-policy

Command Objective This command configures the extended community attribute advertisement policy for specific destination.

The no form of the command removes the extended community attribute advertisement policy for specific destination.

Syntax

```
bgp ecomm-policy <ip-address> <prefixlen > <set-add|set-none|modify>

no bgp ecomm-policy <ip-address> <prefixlen>
```

Parameter Description

- `<ip-address>` - Configures the route prefix on which extended community policy needs to be applied.
- `<prefixlen>` - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges between 1 and 32.
- `set-add` - Sends associated route with configured additive extended-communities only.
- `set-none` - Sends the associated route without any extended-communities.
- `modify` - Strips the associated route with received delete extended communities and adds the configured additive extended communities.

Mode BGP Router Configuration Mode/ Address Family Router Configuration Mode

---

Default modify

Example

```
Your Product(config-router)# bgp ecomm-policy 12.0.0.0 14 set-add
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode
- `show ip bgp extcommunity` – Displays the contents of policy ext-community route tables.

31.42 bgp confederation identifier

Command Objective This command configures the BGP confederation identifier which specifies the confederation to which the autonomous systems belong to. This value ranges between 1 and 4294967295 or 0.1 to 65535.65535.

The no form of the command removes the configured BGP confederation identifier and resets the identifier to its default value.

If this value is already configured to a non-zero value, it must be reset to zero (using no form of the command) before reconfiguring.

When four-byte-asn is enabled, this value ranges between 1 and 4294967295or between 0.1 and 65535.65535.

When four-byte-asn is disabled, this value ranges between 1 and 65535. or between 0.1 and 0.65535.

When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.65535.

Syntax

```
bgp confederation identifier <AS no>

bgp confederation identifier <AS no>
```

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default 0

Example

```
Your Product(config-router)# bgp confederation identifier
1000
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp confed info` – Displays information about confederation feature.
- `address-family` - Enters the router into the address-family router configuration mode.
- `ip bgp four-byte-asn` - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system.
- `bgp asnotation dot` - Changes the output format of BGP ASNs from asplain to asdot notation.

31.43 bgp confederation peers

Command Objective This command configures the Autonomous Systems that belongs to the confederation. The autonomous systems specified in this command are visible internally to a confederation. Each autonomous system is fully meshed within itself. This value ranges between 1 and 4294967295 or 0.1 to 65535.65535.

When four-byte-asn is enabled, this value ranges between 1 and 4294967295or between 0.1 and 65535.65535.

When four-byte-asn is disabled, this value ranges between 1 and 65535. or between 0.1 and 0.65535.

When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.1 to 65535.65535.

The no form of the command removes the Autonomous Systems from the confederation.

Syntax

```
bgp confederation peers <AS no>

no bgp confederation peers <AS no>
```

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default By default no AS will be added to the confederation

☞ This command executes only if the Peer AS number is not equal to BGP Speaker Local AS number.

Example

```
Your Product(config-router)# bgp confederation peers 100
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp confed info` – Displays information about confederation feature.
- `ip bgp four-byte-asn` - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system.
- `bgp asnotation dot` - Changes the output format of BGP ASNs from asplain to asdot notation.

31.44 bgp bestpath med confed

Command Objective This command enables MED comparison among paths learnt from confederation peers. The comparison between MEDs is only made if there are no external autonomous systems in the path. If there is an external autonomous system in the path, then the external MED is passed transparently through the confederation, and the comparison is not made.

The no form of the command disables MED comparison among paths learnt from confed peers and prevent the software from considering the MED attribute in comparing paths.

Syntax

```
bgp bestpath med confed

no bgp bestpath med confed
```

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default In BGP route selection algorithm, MED attributes comparison between two routes originated within the local confederation is disabled.

Example

```
Your Product(config-router)# bgp bestpath med confed
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp confed info` – Displays information about confederation feature.
- `address-family` - Enters the router into the address-family router configuration mode.

31.45 neighbor - password

Command Objective This command enables Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers where each segment sent on the TCP connection between the peers is verified. The MD5 authentication must be configured with the same password on both BGP peers; else, the connection between them will not be made.

The no form of the command resets the TCP-MD5 password set for the peer.

Syntax

```
neighbor <ip-address> password password-string

no neighbor <ip-address> password
```

Parameter Description

- `<ip-address>` - Specifies the IP address of the BGP peer for which the TCP MD5 Authentication password is to be set.
- `password- string` - Configures the TCP MD5 Authentication Password that has to be sent with all TCP packets originated from the peer. This value is a string with the maximum size as 80.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default By default, the MD5 password setting is disabled.

☞ This command executes only if Peer is created

Example

```
Your Product(config-router)# neighbor 10.0.0.2 password
abcdef
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp info` – Displays the general information about BGP protocol.

31.46 address-family

Command Objective This command enters the router into the address-family router configuration mode. Routing information is advertised for IPv4 address family when a BGP session is configured, unless the default advertising is reset.

The no form of the command deletes the peers belonging to the IPV4, IPv6 and VPNv4 address family.

Syntax

```
address-family [ipv4 | ipv6] [vrf <vrf-name>]

no address-family { ipv4 | ipv6} [vrf <vrf-name>]
```

Parameter Description

- `ipv4` - Configures session that carries standard IPv4 address prefixes.
- `ipv6` - Configures session that carries standard IPv6 address prefixes.
- `rip` - Redistributes routes that are learnt by the RIP process, in the BGP routing process.
- `vrf <vrf-name>` - Configures the address-family router configuration for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode BGP Router Configuration Mode

Example

```
Your Product(config-router)# address-family ipv4

Your Product(config-router-af4)#

Your Product(config-router)# address-family ipv6

Your Product(config-router-af6)#
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp` – Displays the BGP related information.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - interval` – Configures neighbor interval.
- `neighbor - timers`– Configures neighbor KeepAlive Time and Hold Time Intervals.
- `neighbor - shutdown` – Disables the Peer session.
- `neighbor – update-source` - Configures the source-address for routing updates and for TCP connection establishment with a peer.

- **neighbor – gateway** - Configures gateway router's address that will be used as nexthop in the routes advertised to the peer.
- **neighbor - activate** – Enables default capabilities for the peer and restarts the connnection to the peer if capabilities negotiated change.
- **neighbor - delay open** - Configures a delay in sending the first OPEN message to the BGP peer for a specific time period.
- **neighbor - maximum prefix** - Configures the maximum number of peers supported by BGP.
- **neighbor - damp-peer-oscillations** - Enables the damp peer oscillation option.
- **neighbor – allow-autostop** - Enables the auto stop option to stop the BGP peer and BGP connection automatically.
- **neighbor – connect-retrycount** - Sets the retry count for the BGP peer.
- **neighbor – transport connection-mode** - Configures the BGP Peer Transport Connection status as active or passive.
- **neighbor - peer-group** – Creates a peer group.
- **tcp-ao mkt key-id - receive-key-id** - Creates a TCP-AO MKT in the BGP instance.
- **neighbor –tcp-ao** - sets BGP peer TCP-AO configurations.
- **neighbor - tcp-ao mkt** - Associates a TCP-AO MKT to the BGP peer.

31.47 bgp graceful-restart

Command Objective This command enables graceful restart capability in router which allows forwarding of data packets to continue along known routes, while the routing protocol information is being restored following a processor switch over. When graceful restart is enabled, peer networking devices are informed, through protocol extensions prior to the event.

The no form of the command disables the graceful restart capability and resets the restart-time or stalepath-time to the default value.

Syntax

```
bgp graceful-restart [restart-time <(1-4096)<seconds>] [stalepath-time <(90-3600)<seconds>]

no bgp graceful-restart [restart-time] [stalepath-time]
```

Parameter Description

- `restart-time<(1-4096)<seconds>` - Configures the estimated time (in seconds) taken for re-establishing a BGP session after restart. The default value for this should be less than or equal to Hold Time carried in open message. This value ranges between 1 and 4096 seconds.
- `stalepath-time<(90-3600)<seconds>` - Configures the Time (in seconds) until which the router retains the stale routes. This value ranges between 90 and 3600 seconds.

Mode BGP Router Configuration Mode

Default

- Graceful Restart is disabled.
- restart-time -90 seconds.
- stalepath-time-150 seconds.
- If those time are default value, it will not display bgp graceful-restart command in the running config.
- When creating/deleting a BGP group, the graceful restart will be enable/disable.

Example

```
Your Product(config-router)# bgp graceful-restart restart-time 33 stalepath 789
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp timers` - Displays the value of BGP timers.

- `show ip bgp info` – Displays the general information about BGP protocol.

31.48 bgp update-delay

Command Objective This command configures the selection deferral time interval. This time interval represents the time (in seconds) until which the router defers its route selection. This value ranges between 60 and 1800 seconds.

This time interval should be configured to provide enough time for all the peers of the restarting speaker to send all the routes to the restarting speaker.

The no form of the command resets the time interval to its default value.

Syntax

```
bgp update-delay <(60-1800)seconds>
no bgp update-delay
```

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default 60 seconds

Example

```
Your Product(config-router)# bgp update-delay 90
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp timers` - Displays the value of BGP timers.
- `address-family` - Enters the router into the address-family router configuration mode.

31.49 restart-support

Command Objective This command enables the graceful restart support. Graceful restart support is provided for both planned and unplanned restart, if the command is executed without any option.

The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent.

The no form of the command disables the graceful restart support.

Syntax

```
restart-support [plannedOnly]
no restart-support
```

Parameter Description

- `plannedOnly` - Supports only the planned restarts (such as restarting a control plane after a planned downtime).

Mode BGP Router Configuration Mode

Default Graceful restart support is disabled.

☞ This command executes only if the graceful restart capability is disabled.

Example

```
Your Product(config-router)# restart-support
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `no bgp graceful-restart` - Disables the graceful restart capability and resets the restart-time or stalepath-time to default value.
- `show ip bgp restartsupport` - Displays the restart support of the BGP.

31.50 restart-reason

Command Objective This command configures the reason for the graceful restart of the BGP router. The reason for restart can be unknown, software upgrade, scheduled restart or switch to redundant router.

The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent.

The no form of the command resets the reason for restart.

Syntax

```
restart-reason [{unknown|softwareRestart|swReloadUpgrade}]

no restart-reason
[{unknown|softwareRestart|swReloadUpgrade}]
```

Parameter Description

- `unknown` - Configures reason for graceful restart of the BGP router as restart due to unplanned events (such as restarting after a crash).
- `softwareRestart` - Configures reason for graceful restart of the BGP router as restart due to restart of software.
- `swReloadUpgrade` - Configures reason for graceful restart of the BGP router as restart due to reload or upgrade of software.

Mode BGP Router Configuration Mode

Default softwareRestart

Example

```
Your Product(config-router)# restart-reason
swReloadUpgrade
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp restartreason` - Displays the restart reason of the BGP.

31.51 distribute-list route-map

Command Objective This command enables route map filtering for inbound or outbound routes and defines the conditions for distributing the routes from one routing protocol to another.

The no form of the command disables inbound filtering for the routes.

Syntax

```
distribute-list route-map <name(1-20)> {in | out}
no distribute-list route-map <name(1-20)> {in | out}
```

This command executes only if Peer is created.

Parameter Description

- `<name(1-20>` - Specifies the name of the Route Map to be used for filtering. This value is a string with the maximum size as 20.
- `in` - Sets filtering for inbound routes.
- `out` - Sets filtering for outbound routes.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default By default, the MD5 password setting is disabled.

Only one route map can be set for inbound or outbound routes. Another route map can be assigned, only if the already assigned route map is disabled.

Example

```
Your Product(config-router)# distribute-list route-map
rmap-test in
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode.

31.52 distance

Command Objective This command enables the administrative distance value which is used as a preference parameter in IP for best route selection (. This value ranges between 1 and 255.

The no form of the command disables the administrative distance.

Syntax

```
distance <1-255> [route-map <name(1-20)>]
no distance [route-map <name(1-20)>]
```

If Routemap is disabled

```
distance <1-255>
no distance
```

Parameter Description

- `route-map <name(1-20)>` - Configures the name of the Route Map for which the distance value should be enabled and set. This value is a string with the maximum size as 20.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

☞ Distance can be set for only one route map. Another route map can be assigned, only if the already assigned route map is disabled.

Example

```
Your Product(config-router)# distance 10 route-map rmap-test
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode.

31.53 clear ip bgp

Command Objective This command resets the BGP connection dynamically for inbound and outbound route policy. The inbound routing tables are updated dynamically or by generating new updates using stored update information.

If the keyword soft and the associated direction are not specified, then this causes hard clear, that is, the BGP session with peer is reset.

Syntax

```
clear ip bgp [vrf <string (32)>] {dampening [<random_str>
<num_str>] | flap-statistics [<random_str> <num_str>] |
{ * | <AS no>| external | ipv4 | ipv6 | <random_str> }
[soft [{in [prefix-filter]|out}]] }
```

Parameter Description

- `vrf <vrf-name>` - Resets the BGP connection for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- `dampening [<random_str><num_str>]` - Clears the dampening related configuration for the bgp.
  - `<random_str>` - Clears damping information for the specified ipv4/ipv6 address.
  - `<num_str>` - Specifies the prefix length of the route. This value ranges between 0 and 128.
- `flap-statistics [<random_str> <num_str>` - Clears the route flap statistics for the bgp.
  - `<random_str>` - Clears flap statistics for the specified ipv4/ipv6 address.
  - `<num_str>` - Specifies the prefix length of the route. This value ranges between 0 and 128.
- `*` - Resets All BGP peers.
- `<AS no>` - Clear peers with the specified AS number. This value ranges between 1 and 4294967295 or 0.1 to 65535.65535.

  When four-byte-asn is enabled, this value ranges between 0 and 4294967295or between 0.0 and 65535.65535

  When four-byte-asn is disabled, this value ranges between 0 and 65535. or between 0.0 and 0.65535

  When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.0 to 65535.65535

- `external` - Clear all external peers.
- `ipv4` - Resets the bgp connection dynamically for all ipv4 address family peers

- **ipv6** - Resets the bgp connection dynamically for all ipv6 address family peers
- **<random_str>** - Resets the bgp connection dynamically for the specified ip address or the configured peer group name.
  - **<ip-address>** - Resets the bgp connection for the specified peer identified with the ip-address.
  - **<peer-group-name>** - Resets the bgp connection dynamically for all the members of the given peer group.
- **soft** - Configures the Soft clear which is automatically assumed when the route refresh capability is supported
  - **in** - Initiates inbound soft reconfiguration which causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy
  - **prefix-filter** - Pushes out prefix-list ORF and initiates inbound soft reconfiguration
  - **out** - Initiates outbound soft configuration which does not have any memory overhead and does not require any preconfiguration. An outbound reconfiguration can be triggered on the other side of the BGP session to make the new inbound policy take effect.

Mode Privileged EXEC Mode

Example

```
Your Product# clear ip bgp dampening 12.0.0.1 0
```

Related Command(s)

- **bgp dampening** – Sets the BGP dampening parameters.
- **ip bgp dampening** - Configures the dampening parameters and changes various BGP route dampening factors.
- **show ip bgp** – Displays the BGP related information.
- **ip bgp four-byte-asn** - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system.
- **bgp asnotation dot** - Changes the output format of BGP ASNs from asplain to asdot notation.

31.54 do shutdown ip bgp

Command Objective This command sets the BGP Speaker Global Admin status DOWN.

The no form of the command sets the BGP Speaker Global Admin status UP. BGP functionally is active only when the global admin status is UP.

The shutdown command does not affect all the configurations. All peer sessions go down and routes learnt through redistribution are lost. If RFD is enabled, then routes history is cleared.

Syntax

```
do shutdown ip bgp [ vrf <vrf-name> ]
no shutdown ip bgp [ vrf <vrf-name> ]
```

Parameter Description

- `vrf <vrf-name>` - Sets the BGP Speaker Global Admin status up / down for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32

Mode Global Configuration Mode

Default The BGP Speaker Global Admin status is DOWN.

The BGP Speaker Global Admin status can be made UP only if the BGP Speaker Local AS Number is configured.

Example

```
Your Product(config)# do shutdown ip bgp
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `ip bgp overlap-policy` – Configures the Overlap Route policy for the BGP Speaker.
- `ip bgp synchronization / synchronization` – Enables synchronization between BGP and IGP.
- `show ip bgp info` – Displays the general information about BGP protocol.

31.55 debug ip bgp

Command Objective This command enables the tracing of the BGP module as per the configured debug levels. The trace statements are generated for the configured trace levels.

The no form of the command disables the tracing of the BGP module as per the configured debug levels. The trace statements are not generated for the configured trace levels.

Syntax

```
debug ip bgp [vrf <vrf-name> ] [{all|ipv4 unicast |ipv6 unicast | <random_str>}] [{peer | update | fdb | keep | in | out | damp | events | gr }]

no debug ip bgp [vrf <vrf-name> ]{peer | update | fdb | keep | in | out | damp | events | gr | all}
```

Parameter Description

- `vrf <vrf-name>` - Generates debug ststements for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- `all` - Generates debug statements for all peers.
- `ipv4 unicast` - Generates debug statements for the trace code related to ipv4 peers or related ipv4 unicast address family peers.
- `ipv6 unicast` - Generates debug statements for the trace code related to ipv6 peers or related ipv6 unicast address family peers.
- `<random_str>` - Generates debug statements for the trace code related for the specified IPv4 or IPv6 peer address.
- `peer` - Generates debug statements forthe trace code related to peer processing.
- `update` - Generates debug statements for the trace code related to update processing
- `fdb` - Generates debug statements for the trace code related to FDB updation.
- `keep` - Generates debug statements for the trace code related to keep-alives.
- `in` - Generates debug statements for the trace code related to incoming messages.
- `out` - Generates debug statements for the Trace code related to outgoing messages.
- `damp` - Generates debug statements for the Trace code related to dampening parameters.
- ---
- `events` - Generates debug statements for the trace code related to BGP event processing.

- `gr` - Generates debug statements for the trace code related to graceful restart.
- `all` - Generates debug statements for all the BGP trace code.

Mode	Privileged EXEC Mode
☞	This command executes only if BGP Speaker local AS number is configured.
Example	`Your Product# debug ip bgp peer`

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.

31.56 show bgp-version

Command Objective	This command displays the BGP Version information.
Syntax	`show bgp-version`
Mode	Privileged EXEC Mode
Default	The BGP Speaker Global Admin status is DOWN.
Example	`Your Product# show bgp-version` `BGP Version : 4`

31.57 show ip bgp

Command Objective This command displays the BGP related information.

Syntax

```
show ip bgp [vrf <vrf-name>]{[neighbor [<peer-addr>
[received prefix-filter]]]| [rib]| [stale]|[<ip_addr>]
[prefix-len]}
```

Parameter Description

- `vrf <vrf-name>` - Sets the BGP Speaker Global Admin status up / down for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- `neighbor <peer-addr>` - Displays BGP information for the specified IP address of the neighbor.
  - `received prefix-filter` - Displays the received ORF entries
- `rib` - Displays the BGP local RIB (Routing Information Base).
- `stale` - Displays the routes which have gone stale due to Graceful restart.
- `<ip addr>` - Displays BGP information for the specified IP address from the RIB.
- `prefix-len` - Displays BGP information for the specified prefix length from the RIB. This value ranges between 0 and 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp neighbor 60.0.0.5
  BGP neighbor is 12.9.9.9, remote AS 23, external link
  BGP version 0, remote router ID 0.0.0.0
  BGP state = Idle
  Configured BGP Maximum Prefix Limit 100
  AutomaticStart DISABLED
  AutomaticStop DISABLED
  DampPeer Oscillations DISABLED
  DelayOpen DISABLED
  Configured Connect Retry Count 5
  Current Connect Retry Count 0
  Default-originate : DISABLED
```

```
Peer Passive : DISABLED

Peer Status : NOT DAMPED

GateWay Address : NONE

Rcvd update before 0 secs, hold time is 90,
keepalive interval is 30 secs

Ip Prefix-list IN: aa

Received 0 messages, 0 Updates

Sent 0 messages, 0 Updates

Route refresh: Received 0, sent 0.

Minimum time between advertisement runs is 30 seconds

Connections established 0 time(s)

Local host: 12.0.0.2, Local port: 0

Foreign host: 12.9.9.9, Foreign port: 0

Last Error: Code 0, SubCode 0.

Update Source 12.0.0.2

Next-Hop is automatic

MultiHop Status - disabled

Send-Community is standard,extended
```

Your Product# show ip bgp rib

```
BGP table version is 1,local router ID is 60.0.0.2

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

Origin codes: i - IGP, e - EGP, ? - incomplete

Type  Network   NextHop     Metric LocPrf Path Origin

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

>    66.0.0.0/8 60.0.0.66/4  0       -       ?
```

Your Product# show ip bgp stale

```
Context Name : default

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

BGP table version is 7,local router ID is 60.0.0.5

Origin codes: i - IGP,e - EGP, ? - incomplete

Network    NextHop     Metric   LocPrf  Path Origin

--------   -------     ------   ------  --------
```

```
66.0.0.0/8 60.0.0.66/4   100        200        ?
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `bgp router-id` – Configures the BGP Identifier of the BGP Speaker.
- `neighbor – remote-as` –Creates a Peer and initiates the connection to the peer.
- `neighbor – interval` – Configures neighbor interval.
- `neighbor – timers`– Configures neighbor KeepAlive Time and Hold Time Intervals.
- `neighbor – shutdown` – Disables the Peer session.
- `neighbor – update-source` - Configures the source-address for routing updates and for TCP connection establishment with a peer.
- `neighbor – gateway` - Configures gateway router's address that will be used as nexthop in the routes advertised to the peer.
- `neighbor – activate` – Enables default capabilities for the peer and restarts the connnection to the peer if capabilities negotiated change.
- `neighbor – delay open` - Configures a delay in sending the first OPEN message to the BGP peer for a specific time period.
- `neighbor – maximum prefix` - Configures the maximum number of eers supported by BGP.
- `neighbor – damp-peer-oscillations` - Enables the damp peer oscillation option.
- `neighbor – allow-autostop` - Enables the auto stop option to stop the BGP peer and BGP connection automatically.
- `neighbor – connect-retrycount` - Sets the retry count for the BGP peer.
- `neighbor – transport connection-mode` - Configures the BGP Peer Transport Connection status as active or passive.
- `neighbor – peer-group` – Creates a peer group.
- `clear ip bgp` –Resets the BGP connection dynamically for inbound and outbound route policy.
- `neighbor – Local-as` - Updates the local AS used for the peer connection.

31.58 show ip bgp restart mode

Command Objective This command displays the restart mode of the BGP router and neighbors.The BGP Speaker can be in restarting or receiving mode.

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax `show ip bgp {restartmode [neighbor [<peer-addr>]]}`

Parameter Description

- `restartmode` - Displays the restart mode fo the BGP router.
- `neighbor <peer-addr>` - Displays the restart mode for the specified IP address of the neighbor.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp restartmode neighbor 10.2.4.5
     Context Name : default
     -------------
     BGP4:- In Receiving Mode
     Neighbor    RestartMode
     ---------   -------
      None
Your Product# show ip bgp restartmode neighbor 23.45.0.1
 Context Name : default
 -------------
 BGP4:- Restart feature is not enabled Neighbor RestartMode
 ---------   -------
 23.45.0.1 None Context Name : vrf1
 -------------
 BGP4:- Restart feature is not enabled Context Name : vrf2
 -------------
 BGP4:- Restart feature is not enabled
```

Related Command(s)

- `bgp graceful-restart` - Enables the graceful restart capability.
- `neighbor – remote-as` – Creates a Peer and initiates the connection to the peer.

31.59 show ip bgp EndOfRIBMarkerStatus

Command Objective This command displays the End_Of_RIB marker status of the BGP router and neighbors.

Syntax

```
show ip bgp [vrf <vrf-name>] {EndOfRIBMarkerStatus
[neighbor [<peer-addr>]]}
```

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Parameter Description

- **vrf <vrf-name>** - Displays the End_Of_RIB marker status for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- **neighbor <peer-addr>** - the End_Of_RIB marker status for the specified IP address of the neighbor.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp EndOfRIBMarkerStatus

     Context Name : default

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

     Neighbor          EORSent          EORRcvd

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

      60.0.0.5.1.1     NA               Received
      30.0.0.4         Sent             Received

Your Product# show ip bgp EndOfRIBMarkerStatus neighbor
60.0.0.5

     Context Name : default

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

     Neighbor          EORSent          EORRcvd

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

     60.0.0.5.1        NA               Received
Your Product# show ip bgp vrf vrf1 EndOfRIBMarkerStatus

     Context Name : vrf1
```

```
-------------
Neighbor          EORSent          EORRcvd
--------          -------          -------
23.45.0.1         NA               NA
```

Related Command(s)

- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.

31.60 show ip bgp restartreason

Command Objective This command displays the restart reason of the BGP.

Syntax `show ip bgp restartreason`

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp restartreason
     Context Name : default
     -------------
     BGP4: Restart reason is software restart
Your Product# show ip bgp restartreason
     Context Name : default
     -------------
     BGP4: Restart reason is software upgrade
Your Product# show ip bgp restartreason
     Context Name : vrf1
     -------------
     BGP4: Restart reason is unknown
```

Related Command(s)

- `restart-reason` - Configures the reason for BGP graceful restart.

31.61 show ip bgp restartexitreason

Command Objective This command displays the restart exit reason of the BGP. This is the outcome of the last attempt at a graceful restart.

The valid exit reasons can be

- None – The speaker has not restarted.
- InProgress - A restart attempt is currently underway.
- Success- A restart is completed successfully.
- Failure - Failure due to the speaker is not completed the restart process within the restart interval.

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax `show ip bgp restartexitreason`

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp restartexitreason
     Context Name : default
     -------------
     BGP4: Restart In Progress
Your Product# show ip bgp restartexitreason
     Context Name : default
     -------------
     BGP4: Restart Speaker hs not restarted
Your Product# show ip bgp restartexitreason
     Context Name : default
     -------------
     BGP4: GR Exit Reason is Success
Your Product# show ip bgp restartexitreason
     Context Name : default
     -------------
     BGP4: GR Exit Reason is Failure
```

Related Command(s)

- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `bgp graceful-restart` - Enables the graceful restart capability.

31.62 show ip bgp restartsupport

Command Objective This command displays the restart support of the BGP.

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax `show ip bgp restartsupport`

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp restartsupport

     BGP4: Both planned and unplanned restart are
     supported

Your Product# show ip bgp restartsupport

     BGP4: Planned restart is supported

Your Product# show ip bgp restartsupport

     BGP4: Speaker does not have restart support
```

Related Command(s)

- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `restart-support` - Enables the graceful restart support.

31.63 show ip bgp restartstatus

Command Objective This command displays the current restart status of the BGP. This indicates if the speaker is restarted or not and if it is restarted whether it is a planned restart or unplanned restart.

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax `show ip bgp restartstatus`

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp restartstatus
     Context Name : default
     -------------
     BGP4: Restart status in none
     Context Name : vrf1
     -------------
     BGP4: Restart status in unplanned
     Context Name : vrf2
     -------------
     BGP4: Restart status in none
```

Related Command(s)

- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `bgp graceful-restart` - Enables the graceful restart capability.

31.64 show ip bgp community-number

Command Objective This command displays routes that belong to specified BGP communities.

Syntax

```
show ip bgp community community-number(4294967041-4294967043,65536-4294901759) [exact]
```

- To execute this command L3VPN flag should be enabled.

Parameter Description

- `community-number(4294967041-4294967043,65536-4294901759)` - Displays the routes that belong to the specified BGP Community attribute. This value ranges between 4294967041 and 4294967043 or between 65536 and 4294901759.
- `exact` - Displays the routes that has the same specified communities.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp community community-number 75000
BGP table version is 5,local router ID is 10.0.0.2
Status codes: d damped * valid, > best, I - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network     Next Hop    Metric LocPrf Path
-------     ---------   -----  ------ ----
76.0.0.0/8   10.0.0.1      1          100
77.0.0.0/8   10.0.0.1      1          100
78.0.0.0/8   10.0.0.1      1          100
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `bgp comm-route` – Configures an entry in additive or delete community table.

31.65 show ip bgp extcommunity – routes

Command Objective This command displays routes that belong to specified BGP extended-communities.

Syntax

```
show ip bgp extcommunity
<value(xx:xx:xx:xx:xx:xx:xx:xx)> [exact]
```

- To execute this command L3VPN flag should be enabled.

Parameter Description

- `<value(xx:xx:xx:xx:xx:xx:xx:xx)>` - Displays the routes for the specified extended community value. This is an octet string value in the form xx:xx:xx:xx:xx:xx:xx:xx.
- `exact` - Displays the routes that has the same specified extended communities.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp show ip bgp extcommunity
01:02:33:33:33:33:33:33
     BGP table version is 5,local router ID is 10.0.0.2
     Status codes: d damped * valid, > best, I - internal
     Origin codes: i - IGP, e - EGP, ? - incomplete
     Network     Next Hop   Metric LocPrf Path
     -------     ---------   -----  ------ ----
     75.0.0.0/8   10.0.0.1      1          100
     79.0.0.0/8   10.0.0.1      1          100
Your Product# show ip bgp extcommunity 01:02:33:33:33:33:33:33
exact
     BGP table version is 5,local router ID is 10.0.0.2
     Status codes: d damped * valid, > best, I - internal
     Origin codes: i - IGP, e - EGP, ? - incomplete
     Network     Next Hop   Metric LocPrf Path
     -------     ---------   -----  ------ ----
     75.0.0.0/8   10.0.0.1      1          100
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `bgp ecomm-route` – Configures an entry in additive or delete extended community table.

31.66 show ip bgp summary

Command Objective This command displays the status of all BGP4 connections. If the VRF option is specified it displays the status of BGP4 connection for the specified VRF instance.

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax `show ip bgp summary [vrf <vrf-name>]`

Parameter Description

- `vrf <vrf-name>` - Displays the status of BGP4 connections for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp summary
Context Name : default
-------------
BGP router identifier is 12.0.0.1, local AS number 1 Forwarding State is enabled
BGP router identifier is 12.0.0.1, local AS number 1
BGP table version is 0
Neighbor      Version       AS     MsgRcvd       MsgSent       Up/Down State/PfxRcd
---------     --------      --     -------       -------       --------------
23.45.0.1     4             66     0             0             Idle
Context Name : vrf1
-------------
BGP router identifier is 0.0.0.0, local AS number 1 Forwarding State is enabled
BGP router identifier is 0.0.0.1, local AS number 1
BGP table version is 0
Neighbor    Version     AS     MsgRcvd  MsgSent    Up/Down State/PfxRcd
 ---------   --------  --     -------  -------     ---------------------
 Context Name : vrf2
 -------------
BGP router identifier is 0.0.0.0, local AS number 1 Forwarding State is enabled
```

```
BGP router identifier is 0.0.0.1, local AS number 1
BGP table version is 0
Neighbor    Version    AS    MsgRcvd  MsgSent   Up/Down State/PfxRcd
---------   --------  --    -------  -------    ---------------------
```

Your Product# show ip bgp summary vrf default

```
Context Name : default
-------------
BGP router identifier is 12.0.0.1, local AS number 1 Forwarding State is enabled
BGP router identifier is 12.0.0.1, local AS number 1
BGP table version is 0
Neighbor    Version    AS    MsgRcvd  MsgSent   Up/Down State/PfxRcd
---------   --------  --    -------  -------    ---------------------
23.45.0.1   4         66       0        0          -   Idle
```

Related Command(s)

- **router bgp** – Sets the AS number of the BGP Speaker.
- **bgp router-id** – Configures the BGP Identifier of the BGP Speaker.
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer.
- **neighbor - peer-group** – Creates a peer group.

31.67 show ip bgp filters

Command Objective This command displays the contents of filter table.

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax `show ip bgp filters [vrf <vrf-name>]`

Parameter Description

- `vrf <vrf-name>` - Displays the contents of filter table.for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp filters
Context Name : default
-------------
Index AdminStatus Remote-AS Prefix PrefixLen Inter-AS  Direction Action
----- ----------- --------- ------ --------- -------- ---
6       up          145     72.93.0.0 16       150     in    filter
Context Name : vrf1
-------------
Index AdminStatus Remote-AS Prefix              PrefixLen Inter-AS  Direction
Action
----- ----------- --------- -------------------- -------- -------- ---------
```

```
Your Product# show ip bgp filters vrf default
Context Name : default
-------------
Index AdminStatus Remote-AS Prefix PrefixLen Inter-AS  Direction Action
----- ----------- --------- ------ --------- -------- ---
6       up          145     72.93.0.0 16       150     in    filter
```

Related Command(s)

- `bgp update-filter` – Configures an entry in Update Filter Table.

31.68 show ip bgp aggregate

Command Objective This command displays the contents of aggregate table.

The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax `show ip bgp aggregate [vrf <vrf-name>]`

ParameterDescription

- `vrf <vrf-name>` - Displays the contents of the aggregate table.for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32·

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp aggregate
    Context Name : default
    ----------------------
    Index AdminStatus   Prefix PrefixLen Advertise
    ----- ------------  ------ --------- ----------
    1       up            10.0.0.0   8     all
    2       up            20.0.0.0   8     summary-only
    3       up            50.0.0.0   8     all
```

Related Command(s)

- `aggregate-address index` – Configures an entry in Aggregate Table.

31.69 show ip bgp med

Command Objective This command displays the contents of MED table.

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax `show ip bgp med [vrf <vrf-name>]`

Parameter Description

- `vrf <vrf-name>` - Displays the contents of MED table.for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp med
Context Name : default
-------------
Index Admin  Remote-AS Prefix PrefixLen Inter-AS  Direction Value PreferenceStatus
-------      --------- ------ --------- --------   --------- ----- -------
5            up         200    212.23.45.0 24150    in       50    true
Context Name : vrf1
-------------
Index Admin  Remote-AS Prefix PrefixLen Inter-AS  Direction Value PreferenceStatus
-------      --------- ------ --------- --------   --------- ----- -------
```

```
Your Product# show ip bgp med default
Context Name : default
-------------
Index Admin  Remote-AS Prefix PrefixLen Inter-AS  Direction Value PreferenceStatus
-------      --------- ------ --------- --------   --------- ----- -------
5            up         200    212.23.45.0 24150    in       50    true
```

Related Command(s)

- `bgp med` – Configures an entry in MED Table.

- `bgp bestpath med confed` – Enables MED comparison among paths learnt from confed peers

31.70 show ip bgp dampening

Command Objective This command displays the contents of Dampening table.

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax

```
show ip bgp dampening [vrf <vrf-name>] [{flap-statistics | dampened-paths}]
```

Parameter Description

- **vrf <vrf-name>** - Displays the contents of Dampening table for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- **flap-statistics** - Displays the flap-statistics contents of Dampening table.
- **dampened-paths** - Displays the dampened-paths contents of Dampening table.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp dampening
     Context Name : default
     --------------
     Half Life Time is 900
     Reuse value is 750
     Suppress value is 2000
     Max Suppress time is 3600
     Decay timer granularity is 1
     Reuse timer granularity is 15
     Reuse index array size is 1024
     Context Name : vrf1
     --------------
     Half Life Time is 1000
     Reuse value is 1998
     Suppress value is 2000
```

```
        Max Suppress time is 3600
        Decay timer granularity is 1
        Reuse timer granularity is 135
        Reuse index array size is 257
        Context Name : vrf2
        --------------
        Half Life Time is 2000
        Reuse value is 1990
        Suppress value is 2050
        Max Suppress time is 3600
        Decay timer granularity is 1
        Reuse timer granularity is 135
        Reuse index array size is 257
Your Product# show ip bgp dampening vrf default
        Context Name : default
        --------------
        Half Life Time is 601
        Reuse value is 750
        Suppress value is 2000
        Max Suppress time is 3600
        Decay timer granularity is 1
        Reuse timer granularity is 15
        Reuse index array size is 1024
Your Product# show ip bgp dampening flap-statistics
        Context Name : default
        --------------
         No routes in BGP Rib
```

Related Command(s)

- **ip bgp dampening** – Configures the Dampening Parameters.
- **bgp dampening** – Configures the Dampening Parameters.

31.71 show ip local-pref

Command Objective This command displays the contents of local preference table.

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax `show ip bgp local-pref [vrf <vrf-name>]`

Parameter Description

- `vrf <vrf-name>` - Displays the contents of local preference table.for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp local-pref
     Context Name : default
     --------------
     Cluster id is    12.0.0.1
     Desired Support of the route reflector - Client
     Support BGP Peer Extension Table
     Peer Address Client/Non-Client
      ---- ------- -----------------
     13.0.0.25    Non-Client
     Context Name : vrf1
     --------------
     Cluster id is    None
     Desired Support of the route reflector - Client
     Support BGP Peer Extension Table
     Peer Address Client/Non-Client
      ---- ------- -----------------
     25.0.0.25    Non-Client
```

```
Your Product# show ip bgp local-pref vrf default

Context Name : default

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

Cluster id is    12.0.0.1

Desired Support of the route reflector - Client
Support

BGP Peer Extension Table

Peer Address Client/Non-Client

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

13.0.0.25    Non-Client
```

Related Command(s)

- `bgp local-preference` – Configures an entry in Local Preference Table.

31.72 show ip bgp timers

Command Objective This command displays the value of BGP timers.

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax `show ip bgp timers [vrf <vrf-name>]`

Parameter Description

- `vrf <vrf-name>` - Displays the value of BGP timers for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp timers
Context Name : default
 -------------
Graceful restart Timers
-------------------------
Restart Time    90
Stale Time      150
Selection Deferral Timer Time      60
                      Peer Timers
Peer Address Holdtime KeepAliveTime ConnectRetry ASOrig IdleHoldTime DelayOpenTime
RouteAdvt RestartTime
    ---- ------- -------- ------------- ------------ -----
   ------------ ------------- --------- ------------
23.45.0.1        90      30            30       15            60              0
30       NA
Context Name : vrf1
-------------
Graceful restart Timers
-------------------------
Restart Time 90
Stale Time 150
```

```
Selection Deferral Timer Time      60

   Peer Timers

   Peer Address Holdtime KeepAliveTime ConnectRetry

ASOrig IdleHoldTime DelayOpenTime RouteAdvt    ---- ------- -------- ------------- --------
---- -----  ------------ ------------- --------- ------------

Context Name : vrf2

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

Graceful restart Timers

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

Restart Time 90

Stale Time 150

Selection Deferral Timer Time      60

   Peer Timers

   Peer Address Holdtime KeepAliveTime ConnectRetry

ASOrig IdleHoldTime DelayOpenTime RouteAdvt RestartTime

 ---- ------- -------- ------------- ------------ ----------------- --------- ------------
```

Your Product# show ip bgp timers vrf default

```
Context Name : default

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

 Graceful restart Timers

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

 Restart Time 90

 Stale Time 150

 Selection Deferral Timer Time      60

   Peer Timers

   Peer Address Holdtime KeepAliveTime ConnectRetry ASOrig IdleHoldTime DelayOpenTime
   RouteAdvt RestartTime

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

   ------------ ------------- --------- ------------
   23.45.0.1        90      30            30       15            60              0

   30       NA
```

Related Command(s)

- **ip bgp dampening** – Configures the Dampening Parameters.
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer.
- **neighbor - interval** – Configures neighbor interval.

- **neighbor - timers** – Configures neighbor KeepAlive Time and Hold Time Intervals.
- **neighbor - peer-group** – Creates a peer group.
- **bgp graceful-restart** - Enables the graceful restart capability.
- **bgp update-delay** - Configures the selection deferral time interval.

31.73 show ip bgp info

Command Objective This command displays the general information about BGP protocol.

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax `show ip bgp info [vrf <vrf-name>]`

Parameter Description

- `vrf <vrf-name>` - Displays the general information about BGP protocol for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp info

     Context Name : default

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

     Routing Protocol is "bgp
     1" Bgp Trap : Enabled

     The route change interval is "60"
     IGP synchronization is enabled

     Both more-specific and less-specific overlap route
     policy is set
   Administrative Distance is 122

   Default IPv4 Unicast Capability Status is set

   Local Preference is 100

     Non-bgp routes are advertised to bothexternal and
     internal peers

   MED Comparision is disabled

   Metric is 0

   Default Originate Disable

   Redistributing:
```

```
     BGP GR admin status is disabled
    Maximum paths: ibgp - 1 ebgp -      1 eibgp - 64
    Maximum paths (Operational): ibgp - 1 ebgp -  1 eibgp -
    1
    Peer Table
Peer Address RemoteAS NextHop   MultiHop  Send-
---- ------- -------- ------- -------- -------------------
23.45.0.1    66     self       enable    standard,extended
      Context Name : vrf1
      -------------
         Routing Protocol is "bgp 1"
         Bgp Trap : Enabled
         The route change interval is "60"
         IGP synchronization is enabled
         Both more-specific overlap route policy is set
         Administrative Distance is 122
         Default IPv4 Unicast Capability Status is set
         Local Preference is 100
      Non-bgp routes are advertised to bothexternal and
      internal peers
         MED Comparision is disabled
         Metric is 0
         Default Originate Enable
         Redistributing:
          BGP GR admin status is disabled
         Maximum paths: ibgp - 1 ebgp -      1 eibgp - 64
         Maximum paths (Operational): ibgp - 1 ebgp -  1
        eibgp - 1
         Peer Table
 Peer Address RemoteAS NextHop   MultiHop  Send-community
  ---- ------- -------- ------- -------- -------------------
      Context Name : vrf2
      -------------
         Routing Protocol is "bgp 1"
         Bgp Trap : Enabled
         The route change interval is "60"
         IGP synchronization is enabled
```

```
                Both more-specific overlap route policy is set
                Administrative Distance is 122
                Default IPv4 Unicast Capability Status is set
                Local Preference is 100
              Non-bgp routes are advertised to bothexternal and
              internal peers
                MED Comparision is disabled
                Metric is 0
                Default Originate Enable
                Redistributing:
                 BGP GR admin status is disabled
                Maximum paths: ibgp - 1 ebgp -      1 eibgp - 64
                Maximum paths (Operational): ibgp - 1 ebgp -   1
              eibgp - 1
                Peer Table
Peer Address RemoteAS NextHop   MultiHop  Send-community
  ---- ------- -------- ------- -------- ------------------
       Your Product# show ip bgp info vrf default
            Context Name : default
             -------------
            Routing Protocol is "bgp
            1" Bgp Trap : Enabled
            The route change interval is "60"
            IGP synchronization is disabled
              More-specific overlap route policy is set
           Administrative Distance is 122
           Default IPv4 Unicast Capability Status is set
           Local Preference is 100
             Non-bgp routes are advertised to bothexternal and
             internal peers
           MED Comparision is disabled
           Metric is 0
           Default Originate Disable
           Redistributing:
            BGP GR admin status is disabled
           Maximum paths: ibgp - 1 ebgp -      1 eibgp - 64
```

```
Maximum paths (Operational): ibgp - 1 ebgp -  1 eibgp -
1

Peer Table

Peer Address RemoteAS NextHop    MultiHop  Send-community
---- ------- -------- ------- -------- ------------------
60.0.0.5     500      automatic disable standard,extended
```

Related Command(s)

- **router bgp** – Sets the AS number of the BGP Speaker.
- **ip bgp overlap-policy** – Configures the Overlap Route policy for the BGP Speaker.
- **default-information originate** - enables redistribution and advertisement of the default router.
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer.
- **neighbor - peer-group** – Creates a peer group.
- **ip bgp synchronization / synchronization** – Enables synchronization between BGP and IGP.
- **bgp default local-preference** – Configures the Default Local Preference value.
- **neighbor - ebgp-multihop** – Enables BGP to establish connection with external peers.
- **neighbor - next-hop-self** – Enables BGP to send itself as the next hop for advertised routes.
- **neighbor - interval** – Configures neighbor interval r.
- **neighbor - activate** – Enables default capabilities for the peer and restarts the connnection to the peer if capabilities negotiated change.
- **neighbor - send-community** – Enables advertisement of community attributes to (standard/extended) peer.
- **neighbor - timers** – Configures neighbor KeepAlive Time and Hold Time Intervals.
- **bgp nonbgproute-advt** – Controls the advertisement of Non-BGP routes.
- **redistribute** – Configures the protocol from which the routes have to be redistributed into BGP.
- **bgp always-compare-med** – Enables the comparison of med for routes received from different autonomous system.
- **default-metric** – Configures the Default IGP Metric value
- **neighbor** - password – Configures the password for TCP-MD5 authentication with peer.

- **bgp graceful-restart** - Enables the graceful restart capability.
- **do shutdown ip bgp** – Sets the BGP Speaker Global Admin status DOWN.
- **bgp trap** - Enables /disables the bgp trap notification.
- **nexthop processing-interval** - Configures the interval at which next hops are monitored for reachablity.
- **redistribute ospf** - Configures the OSPF protocol from which the routes are redistributed into BGP.
- **maximum-paths** - Sets the BGP multipath count.

31.74 show ip rfl info

Command Objective This command displays information about Route Reflector feature.

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax `show ip bgp rfl info [vrf <vrf-name>]`

Parameter Description

- `vrf <vrf-name>` - Displays the information about Route Reflector feature for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp rfl info
     Context Name : default
     --------------
     Cluster id is    12.0.0.1
     Desired Support of the route reflector - Client
      Support BGP Peer Extension Table

      Peer Address Client/Non-Client
      ---- ------- -----------------
      23.45.0.1      Non-Client
     Context Name : vrf1
     --------------
     Cluster id is    None
     Desired Support of the route reflector - Client
      Support BGP Peer Extension Table

      Peer Address Client/Non-Client
      ---- ------- -----------------
Your Product# show ip bgp rfl info vrf default
```

```
Context Name : default

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

Cluster id is    12.0.0.1

Desired Support of the route reflector - Client
Support

BGP Peer Extension Table

 Peer Address Client/Non-Client

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

 23.45.0.1    Non-Client
```

Related Command(s)

- **bgp nonbgproute-advt** – Controls the advertisement of Non-BGP routes either to the external peer (1) or both to internal & external peer (2)
- **bgp client-to-client reflection** – Configures the Route Reflector to support route reflection to Client Peers.
- **neighbor - route-reflector-client** – Configures the Peer as Client of the Route Reflector.
- **bgp cluster-id** – Configures the Cluster ID for Route Reflector.

31.75 show ip bgp confed info

Command Objective This command displays information about confederation feature.

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax `show ip bgp confed info [vrf <vrf-name>]`

Parameter Description

- `vrf <vrf-name>` - Displays the information about confederation feature for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp confed info
     Context Name : default
     --------------
     Confederation Identifier is 1000
     Confederation best path med comparision is set
     Confederation peers: 100
     Context Name: vrf1
     --------------
     Confederation Identifier is 0
     Confederation best path med comparision is not set
     Confederation peers: None
     Context Name: vrf2
     --------------
     Confederation Identifier is 0
     Confederation best path med comparision is not set
     Confederation peers: None
```

```
Your Product# show ip bgp confed info vrf default
     Context Name : default
     -------------
     Confederation Identifier is 1000
     Confederation best path med comparision is set
     Confederation peers: 100
```

Related Command(s)

- **bgp confederation identifier** – Configures the BGP confederation identifier.
- **bgp bestpath med confed** – Enables MED comparison among paths learnt from confed peers.
- **bgp confederation peers** – Configures the Autonomous Systems that belongs to the confederation.

31.76 show ip bgp community

Command Objective This command displays the contents of community tables.

- The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax

```
show ip bgp community [vrf <vrf-name>]
{route|policy|filter}
```

Parameter Description

- `vrf <vrf-name>` - Displays contents of community tables for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- `route` - Displays the entry in additive or delete community table.
- `policy` - Displays the Community attribute advertisement policy for specific destination.
- `filter` - Displays the filter community attribute while receiving or advertising.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp community route
    Context Name : default
    --------------
    Additive Community Table
     Prefix          PrefixLen     AddCommVal
     -----          ---------     ----------
     30.0.0.0          8           70000
     60.0.0.0          8           75000
     75.0.0.0          8           70000
     76.0.0.0          8           75000
     77.0.0.0          8           75000
     78.0.0.0          8           75000
```

```
 78.0.0.0        8         76000

Delete Community Table

 Prefix        PrefixLen    DeleteCommVal

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

 40.0.0.0        8         80000

 70.0.0.0        8         85000
```

Your Product# show ip bgp community filter

```
Context Name : default

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

Incoming Filter Table

 CommValue  FilterStatus

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

 70000      accept

 80000      deny

Outgoing Filter Table

CommValue  FilterStatus

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

 75000      accept

 80000      deny
```

Your Product# show ip bgp community policy

```
Context Name : default

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

Community Policy Table

 Prefix        PrefixLen    SendStatus

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

 20.0.0.0        8         set-add

 30.0.0.0        8         set-none
```

```
40.0.0.0          8          modify
```

Related Command(s)

- **bgp comm-route** – Configures an entry in additive or delete community table.
- **bgp comm-filter** – Allows/filters the community attribute while receiving or advertising.
- **bgp comm-policy** – Configures the community attribute advertisement policy for specific destination.

31.77 show ip bgp extcommunity

Command Objective This command displays the contents of extended -community tables.

The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax

```
show ip bgp [vrf <vrf-name>] extcommunity
{route|policy|filter}
```

Parameter Description

- `vrf <vrf-name>` - Displays the contents of extended -community tables for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- `route` - Displays the entry in additive or delete ext community table.
- `policy` - Displays the extended community attribute advertisement policy for specific destination.
- `filter` - Displays the extended community filters attribute while receiving or advertising.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp extcommunity route
     Context Name : default
     --------------
     Additive Ext-Community Table
      Prefix        PrefixLen    AddECommVal
      -----         ---------    ------------
      30.0.0.0          8          1:1:22:33:44:55:66:77
      60.0.0.0          8          1:1:22:33:44:55:66:88
      75.0.0.0          8          1:1:33:33:33:33:33:33
      76.0.0.0          8          1:2:44:33:33:33:33:33
      78.0.0.0          8          1:2:33:33:33:33:33:33
      78.0.0.0          8          1:2:33:33:33:33:33:44
```

```
 79.0.0.0        8         1:2:33:33:33:33:33:44

 79.0.0.0        8         1:2:33:33:33:33:33:33

Delete Ext-Community Table

 Prefix        PrefixLen    DeleteECommVal

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

 40.0.0.0        8         80000

 70.0.0.0        8         85000

Context Name : vrf1

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

Additive Ext-Community Table

 Prefix        PrefixLen    AddECommVal

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

Delete Ext-Community Table

 Prefix        PrefixLen    DeleteECommVal
```

Your Product# show ip bgp extcommunity filter

```
Context Name : default

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

Incoming Filter Table

EcommValue            FilterStatus

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

1:1:22:33:44:55:34:77     deny

1:1:22:33:44:55:66:77     accept

Outgoing Filter Table

 EcommValue           FilterStatus

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

 1:1:22:33:44:55:99:77    accept

 1:1:44:33:77:66:99:56    deny
```

```
Your Product# show ip bgp extcommunity policy
     Context Name : default
     --------------
     Ecommunity Policy Table
      Prefix        PrefixLen    SendStatus
      -----         ---------    ----------
      20.0.0.0          8          set-add
      30.0.0.0          8          set-none
      40.0.0.0          8          modify
```

Related Command(s)

- **bgp ecomm-route** – Configures an entry in additive or delete ext community table.
- **bgp ecomm-filter** – Allows/filters the ext community attribute while receiving or advertising.
- **bgp ecomm-policy** – Configures the extended community attribute advertisement policy for specific destination.

31.78 neighbor – maximum-prefix

Command Objective This command configures the maximum number of peers supported by BGP. BGP speaker imposes a locally-configured, upper bound on the number of address prefixes the speaker is willing to accept from a neighbor.

The no form of the command resets the max number of routes that is learned from that particular peer.

Syntax

```
neighbor <ip-address|peer-group-name> maximum-prefix <prefix-limit>

no neighbor <ip-address|peer-group-name> maximum-prefix
```

Parameter Description

- `<ip-address>` - Configures the remote BGP peer IP address for which the maximum peer is to be set.
- `<peer-group-name>` - Specifies the name of the BGP peer group for which the maximum peer is to be set. The members of the peer group will inherit the characteristic configured with this command.
- `maximum-prefix <prefix-limit>` - Configures the maximum number of address prefixes that the BGP Peer is willing to accept from the neighbor. This value ranges between 1 and 5000.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 100

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 maximum-prefix 255
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.

- `show ip bgp neighbor` – Displays neighbor related information for the peer.

31.79 neighbor – connect-retry-count

Command Objective This command sets the retry count for the BGP peer. This counter denotes the number of times the BGP Peer should try to establish a TCP-Connect issue with its neighboring peers. The default value for the counter is set as 5. If the BGP Peer exceeds the maximum count value, automatic stop event takes place and the BGP Peer is brought down to the Idle State.

The no form of the command resets the retry count of the BGP peer.

Syntax

```
neighbor <ip-address|peer-group-name> connect-retry-count <value(1-50)>

no neighbor <ip-address|peer-group-name> connect-retry-count
```

Parameter Description

- `<ip-address>` - Configures the remote IP address of the BGP peer for which the retry count is to be set.
- `<peer-group-name>` - Specifies the name of the BGP peer group for which the retry count is to be set. The members of the peer group will inherit the characteristic configured with this command.
- `connect-retry-count <value(1-50)>` - Configures the retry count which specifies the number of times the BGP peer should try to establish a TCP-connect issue with its neighboring peers. If the BGP Peer exceeds the maximum count value, automatic stop event takes place and the BGP Peer is brought down to the Idle State. This value ranges between 1 and 50.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 5

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 12.0.0.1 connect-retry-count 50
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.

- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.
- `as-num` - Sets the AS (Autonomous System) number for the router.
- `router-id` - Sets the router ID's address for the router.

31.80 neighbor – allow-autostop

Command Objective This command enables the auto stop option to stop the BGP peer and BGP connection automatically.

The no form of this command disables the auto stop option.

Syntax

```
neighbor <ip-address|peer-group-name> allow-autostop
no neighbor <ip-address|peer-group-name> allow-autostop
```

Parameter Description

- `<ip-address>` - Configures the remote IP address of the BGP peer for which the auto stop option is set.
- `<peer-group-name>` - Specifies the name of the BGP peer group for which the auto stop option is set. The members of the peer group will inherit the characteristic configured with this command.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Auto stop option is disbaled.

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 12.0.0.1 allow-autostop
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

31.81 neighbor - damp-peer-oscillations

Command Objective This command enables the damp peer oscillation option On implementing this logic, it damps the oscillations of BGP peers in the face of sequences of automatic start and automatic stop in the IDLE state.

The no form of this commnd disables the damp peer oscillation option.

Syntax

```
neighbor <ip-address|peer-group-name> damp-peer-oscillations

no neighbor <ip-address|peer-group-name> damp-peer-oscillations
```

Parameter Description

- `<ip-address>` - Configures the remote IP address of the BGP peer for which the damp peer oscillation option is set.
- `<peer-group-name>` - Specifies the name of the BGP peer group for which the damp peer oscillation option is set. The members of the peer group will inherit the characteristic configured with this command.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Damp peer oscillation option is disbaled.

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 12.0.0.1 damp-peer-oscillations
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

31.82 neighbor delay-open

Command Objective This command configures a delay in sending the first OPEN message to the BGP peer for a specific time period.

The no form of the command disables the delay open option.

Syntax

```
neighbor <ip-address|peer-group-name> delay-open
no neighbor <ip-address|peer-group-name> delay-open
```

Parameter Description

- `<ip-address>` - Configures the remote IP address of the BGP peer for which the delay open option is set.
- `<peer-group-name>` - Specifies the name of the BGP peer group for which the delay open option is set. The members of the peer group will inherit the characteristic configured with this command.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Delay open option is disbaled.

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 12.0.0.1 delay-open
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

31.83 bgp trap

Command Objective This command enables or disables the bgp trap notification.

Syntax

```
bgp trap <enable|disable>
```

Parameter Description

- `enable` - Enables the trap notification for the BGP system. When there is any change in the graceful restart state of the router or peer, the BGP system sends the notification messages to the SNMP manager. For every graceful restart, appropriate trace messages is generated.
- `disable` - Disables the trap notification for the BGP system and does not send the notification messages to the SNMP manager.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default enable.

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product (config-router)# bgp trap enable
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp info` – Displays the general information about BGP protocol.

31.84 neighbor – peer group

Command Objective This command creates a peer group with the specified peer group name. This value is a string with the maximum size as 20.

The no form of the command deletes the peer group.

Syntax

```
neighbor <peer-group-name> peer-group
no neighbor <peer-group-name> peer-group
```

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Delay open option is disbaled.

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor a1 peer-group
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor <ip-address> peer-group` – Adds the neighbor as a member of the specified peer group.
- `neighbor - activate` – Enables default capabilities for the peer and restarts the connnection to the peer if capabilities negotiated change.
- `neighbor - ebgp-multihop` – Enables BGP to establish connection with external peers.
- `neighbor - next-hop-self` – Enables BGP to send itself as the next hop for advertised routes.
- `neighbor - interval` – Configures neighbor interval.
- `neighbor - timers`– Configures neighbor KeepAlive Time and Hold Time Intervals.
- `neighbor - shutdown` – Disables the Peer session.
- `neighbor - default-originate` - Enables advertisement of the default route to the peer.
- `neighbor - send-community` – Enables advertisement of community attributes to (standard/extended) to peer.

- **neighbor – capability** - Enables the specific BGP capability to be advertised and received from the peer.
- **neighbor delay open** - Configures a delay in sending the first OPEN message to the BGP peer for a specific time period.
- **neighbor damp-peer-oscillations** - Enables the damp peer oscillation option.
- **neighbor maximum prefix** - Configures the maximum number of peers supported by BGP.
- **neighbor – allow-autostop** - Enables the auto stop option to stop the BGP peer and BGP connection automatically.
- **neighbor – transport connection-mode** - Configures the BGP Peer Transport Connection status as active or passive.
- **neighbor – connect-retrycount** - Sets the retry count for the BGP peer.
- **show ip bgp peer-group** – Displays information abouty the peer group.
- **address-family** - Enters the router into the address-family router configuration mode.

31.85 neighbor delay-open

Command Objective This command configures a delay in sending the first OPEN message to the BGP peer for a specific time period.

The no form of the command disables the delay open option.

Syntax

```
neighbor <ip-address|peer-group-name> delay-open
no neighbor <ip-address|peer-group-name> delay-open
```

Parameter Description

- `<ip-address>` - Configures the remote IP address of the BGP peer for which the delay open option is set.
- `<peer-group-name>` - Specifies the name of the BGP peer group for which the delay open option is set. The members of the peer group will inherit the characteristic configured with this command.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Delay open option is disbaled.

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 12.0.0.1 delay-open
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

31.86 neighbor <ip-address> peer-group

Command Objective This command configures a delay in sending the first OPEN message to the BGP peer for a specific time period.

The no form of the command disables the delay open option.

Syntax

```
neighbor <ip-address> peer-group <peer-group-name>
no neighbor <ip-address> peer-group <peer-group-name>
```

Parameter Description

- `<ip-address>` - Specifies the IP address of the peer/ neighbor to be added/ removed from the peer group.
- `<peer-group-name>` - Specifies the peer groujp name to which the neighbor is to be added/ removed.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mod

---

☞ This command executes only if

- Peer is created and Peer AS is configured.
- Peer Group is created.

Example

```
Your Product(config-router)# neighbor 10.3.4.5 peer-group a1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

31.87 neighbor – routemap

Command Objective This command enables routemap or IP prefix list for the neighbor.

The no form of the command disables routemap or IP prefix list for the neighbor.

Syntax

```
neighbor <ip-address|peer-group-name> { route-map <name(1-20)> | prefix-list <ipprefixlist_name(1-20)>} {in | out}

no neighbor <ip-address|peer-group-name> { route-map <name(1-20)> | prefix-list <ipprefixlist_name(1-20)>} {in | out}
```

Parameter Description

- `<ip-address>` - Enables/ Disables Routemap or IP Prefix List for the specified BGP peer's remote IP address.
- `<peer-group-name>` - Enables/ Disables Routemap for the specified BGP peer group. This value is a string with the maximum size as 20.
- `route-map <name(1-20)>` - Specifies the name of the Route Map. This value is a string with the maximum size as 20.
- `prefix-list <ipprefixlist_name> -` Configures IP prefix list for neighbor. This value is a string with the maximum size as 20.
- `in` - Enables/ Disables Routemap or IP Prefix List for inbound routes.
- `out` - Enables/ Disables Routemap or IP Prefix List for outbound routes.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

☞ This command executes only if Peer/ Peer Group is created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 10.3.4.5 route-map r1 in
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.

- **`show ip bgp neighbor`** – Displays neighbor related information for the peer.

31.88 neighbor - transport connection-mode

Command Objective This command configures the BGP Peer Transport Connection status as active or passive.

Syntax

```
neighbor <ip-address|peer-group-name> transport
connection-mode <active | passive>
```

Parameter Description

- `<ip-address>` - Configures the transport connection status for the specified BGP peer's remote IP address.
- `<peer-group-name>` - Specifies name of the BGP peer group for which the transport connection mode is set. The members of the peer group will inherit the characteristic configured with this command.
- `active` - Sets the BGP peer as active. When a peer transport connection is made active, then the peer will immediately initiate the session with the peer by sending an open message to it.
- `passive` - Sets the BGP peer as passive. When the peer transport connection is passive, then the peer will not immediately initiate the session, instead, it waits for the peer to send the open message so that it can respond to it to create the session.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Auto stop option is disbaled.

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 12.0.0.1 allow-
autostop
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `neighbor - peer-group` – Creates a peer group.
- `address-family` - Enters the router into the address-family router configuration mode.

- **`show ip bgp neighbor`** – Displays neighbor related information for the peer.

31.89 nexthop processing-interval

Command Objective	This command configures the interval at which next hops are monitored for reachablity. This value ranges between 1 and 120.
Syntax	`nexthop processing-interval <Next-Hop-Processing-Interval(1-120)>`
Mode	BGP Router Configuration Mode / Address Family Router Configuration Mode
Default	60
Example	`Your Product(config)# nexthop processing-interval 100`

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp info` – Displays the general info about BGP protocol.

31.90 bgp redistribute internal

Command Objective This command enables IBGP routes to be redistributed to other IGP protocols.

The no form of the command disables IBGP routes to be redistributed to other IGP protocols.

Syntax

```
bgp redistribute-internal
no bgp redistribute-internal
```

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default IBGP route redistribution is disabled

Example

```
Your Product(config-router)# bgp redistribute-internal
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `show ip bgp info` – Displays the general info about BGP protocol.

31.91 show ip bgp peer-group

Command Objective This command displays information about the peer group.

The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax

```
show ip bgp [vrf <vrf-name>] peer-group [<peer-group-name> [summary]]
```

Parameter Description

- `vrf <vrf-name>` - Displays information about the peer group for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- `<peer-group-name>` - Displays information for the specified BGP Peer group.
- `summary` - Dsiplays the summary of the peer group neighbors.

Mode Privileged EXEC Mode

This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product# show ip bgp peer-group
Context Name : default
-------------
BGP peer-group is a1, Remote AS 1 BGP Version 0
For address family: IPv4 Unicast
BGP neighbor is a1,peer-group internal, members: 12.3.3.3
BGP Maximum Prefix Limit: 2
Connect Retry Count: 2
Peer Passive :Enabled
Damp Peer oscillatios:Enabled
Rfl Status :Non Client
In Route Map: n1
```

```
Out Route Map: -
Your Product# show ip bgp peer-group summary
Context Name : default
-------------
BGP router identifier is 12.0.0.2, local AS number 1
Forwarding State is enabled
BGP table version is 0
Neighbor  Version  AS  MsgRcvd  MsgSent  Up/Down  State/PfxRcd
--------  -------  --  -------  -------  -------  ------------
12.3.3.3    4       1         0         0       -       Connect
```

Related Command(s)

- **neighbor <ip-address> peer-group** – Adds the neighbor as a member of the specified peer group.
- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer.
- **neighbor - peer-group** – Creates a peer group.
- **neighbor - activate** – Enables default capabilities for the peer and restarts the connnection to the peer if capabilities negotiated change.
- **neighbor - ebgp-multihop** – Enables BGP to establish connection with external peers.
- **neighbor - next-hop-self** – Enables BGP to send itself as the next hop for advertised routes.
- **neighbor - shutdown** – Disables the Peer session.
- **neighbor delay open** - Configures a delay in sending the first OPEN message to the BGP peer for a specific time period.
- **neighbor damp-peer-oscillations** - Enables the damp peer oscillation option.
- **neighbor maximum prefix** - Configures the maximum number of peers supported by BGP.
- **neighbor – allow-autostop** – Enables the auto stop option to stop the BGP peer and BGP connection automatically.
- **neighbor – transport connection-mode** - Configures the BGP Peer Transport Connection status as active or passive.
- **neighbor – connect-retrycount** – Sets the retry count for the BGP peer.

- `neighbor – local-as` - Updates the local AS used for the peer connection.

31.92 redistribute ospf

Command Objective This command configures the OSPF protocol from which the routes are redistributed into BGP.

The no form of the command disables the redistribution of routes from the given OSPF protocol into BGP. The route map is disassociated from the redistribution, if the no form of the command specifies the route map.

Syntax

```
redistribute ospf [match {external | internal | nssa-external}] [route-map <string>] [metric <integer>]

no redistribute ospf [match {external | internal | nssa-external}] [route-map <string>] [metric <integer>]
```

Parameter Description

- `match {external | internal | nssa-external}` - Matches the OSPF route type to be redistributed into BGP, This object is used only during ospf redistribution. The list contains;
  - `external` - Redistributes OSPF external routes.
  - `internal` - Redistributes OSPF internal routes.
  - `nssa-external` - Redistributes OSPF NSSA external routes.
- `route-map <string(20)>` - Identifies the specified route-map in the list of route-maps during redistribution of routes to BGP. If this is not specified, all routes are redistributed. This value is a string with the maximum size as 20.
- `metric <integer>` - Specifies the metric value for the protocol srecified. This value ranges between 0 and 4294967295. If the metric value not specified, default metric value is considered.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default

- Redistribution is disabled
- Metric - 0

☞

- Redistribution can be configured for only one route map.
- Another route map can be assigned, only if the already assigned route map is disabled.

Example

```
Your Product(config-router)# redistribute ospf match
external route-map rm metric 500
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

31.93 neighbor – local-as

Command Objective This command updates the local AS used for the peer connection.

The no form of the command resets the local AS used for the peer connection to the global local-As.

Syntax

```
neighbor <ip-address|peer-group-name> local-as <AS no>
no neighbor <ip-address|peer-group-name> local-as
```

Parameter Description

- `<ip-address>` - Updates the local-as for the IP address of the peer used for the peer connection.
- `<peer-group-name>` - Updates the local-as for the peer group name to which the neighbor is to be added/ removed.
- `local-as <AS no>` - Configures the Autonomous system number for the specified ip address of the peer / peer group name. This value ranges between 1 and 4294967295 or 0.1 to 65535.65535.

  When four-byte-asn is enabled, this value ranges between 0 and 4294967295or between 0.0 and 65535.65535

  When four-byte-asn is disabled, this value ranges between 0 and 65535. or between 0.0 and 0.65535

  When bgp asnotation is enabled, the AS number of the BGP Speaker is displayed in the range 0.0 to 65535.65535

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default Auto stop option is disbaled.

☞ This command executes only if Peer/ Peer Groupis created and Peer AS is configured.

Example

```
Your Product(config-router)# neighbor 10.3.4.5 local-as 1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.

- **neighbor - remote-as** – Creates a Peer and initiates the connection to the peer.
- **neighbor - peer-group** – Creates a peer group.
- **address-family** - Enters the router into the address-family router configuration mode.
- **show ip bgp neighbor** – Displays neighbor related information for the peer.
- **show ip bgp peer-group** - Displays information about the peer group.
- **ip bgp four-byte-asn** - Enables 4-byte ASN support in BGP or in the specified vrf instance created in the system.
- **bgp asnotation dot** - Changes the output format of BGP ASNs from asplain to asdot notation.

31.94 maximum-paths

Command Objective This command sets the BGP multipath count. This is the maximum number BGP multipath routes to be added per destination network in the routing table.

This configuration is effective only after hard/soft reset

The no form of the command resets the bgp multipath count to its default value.

If the no command is executed without the parameter ibgp/eibgp , the maximum path count is set to the default value 1 only for ebgp.

Syntax

```
maximum-paths [{ibgp |eibgp}] <maximum path>
no maximum-paths [{ibgp |eibgp}]
```

Parameter Description

- `ibgp` - Sets the maximum number of internal bgp multipath routes to be added per destination network in the routing table.
- `eibgp` - Sets the maximum number of external plus internal BGP multipath routes (with same AS PATH) to be added per destination network in Routing table.
- `<maximum path>` - Configures the maximum path count for the specified ibgp/ eibgp. This value ranges between 1 and 64.

If this is set to 1, only the best route is added to the forwarding table.

If the command is executed without the parameter ibgp/eibgp, the maximum path count is configured for ebgp.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default 1

Example

```
Your Product(config-router)# maximum-paths eibgp 1
Your Product(config-router-af4)# maximum-paths ibgp 1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.

- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp info` – Displays the general information about BGP protocol.

31.95 tcp-ao mkt key-id - receive-key-id

Command Objective This command creates a TCP-AO Master Key Tuple (MKT) in the BGP instance.

The no form of the command deletes a TCP-AO MKT in the BGP instance.

Syntax

```
tcp-ao mkt key-id <Key Id(0-255)> receive-key-id <Rcv Key Id (0-255)> algorithm {hmac-sha-1 | aes-128-cmac} key <master-key> [tcp-option-exclude]

no tcp-ao mkt key-id <Key Id(0-255)>
```

Parameter Description

- `key-id <Key Id(0-255)>` - Configures the send KeyID of the MKT. This value is used to fill the key-id field in the TCP-AO option in the TCP header. This value ranges between 0 and 255.
- `receive-key-id <Rcv Key Id (0-255)>` - Configures the Receive Key-id of the MKT. The MKT ready at the sender to be used for authenticating received segments is indicated to the peer by filling the receive key id of the MKT in of the TCP-AO option in TCP header. This value ranges between 0 and 255.
- `algorithm {hmac-sha-1 | aes-128-cmac}` - Configures the algorithm used for TCP-AO MAC or KDF calculation.
  - `hmac-sha-1` - Sets the algorithm type as hmac-sha-1.
  - `aes-128-cmac` - Sets the algorithm type as aes-128-cmac.

    This algorithm type is currently not supported
- `key <master-key>` - Configures the master key corresponding to the MKT. This value is an octet string with the size between 1 and 80.
- `tcp-option-exclude` - Sets the exclude TCP optionwhich excludes the TCP options other than TCP-AO during MAC calculation, If this is not set TCP-AO MAC will be calculated on TCP segment including all other TCP options.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default algorithm - hmac-sha-1

This command executes only if BGP Speaker Local AS number is configured.

Example

```
Your Product(config-router)# tcp-ao mkt key-id 1 receive-key-id 1 algorithm  hmac-sha-1 key key1
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - tcp-ao` - sets BGP peer TCP-AO configurations.
- `neighbor - tcp-ao mkt` - Associates a TCP-AO MKT to the BGP peer.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp - tcp-ao mkt summary` - Displays the BGPrelated TCP-AO MKT information

31.96 neighbor - tcp-ao

Command Objective This command sets TCP-AO configurations for the specified BGP Peer.

The no form of the command deletes TCP-AO configurations for the specified BGP peer.

Syntax

```
neighbor <ip-address> tcp-ao { icmp-accept | no-mkt-match packet-discard}

no neighbor <ip-address> tcp-ao { icmp-accept | no-mkt-match packet-discard}
```

Parameter Description

- `<ip-address>` - Configures the BGP peer for which the TCP-AO configurations are done.
- `icmp-accept` -. Accepts ICMPv4 type 3 & ICMPv6 type 1 messages for the TCP-AO authenticated peer.
- `no-mkt-match packet-discard` - Discards packet for the peer, if packets are received with TCP-AO and no matching MKT is found.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

Default Auto stop option is disbaled.

☞ This command executes only if BGP Speaker Local AS number and peer is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 tcp-ao icmp-accept
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `tcp-ao mkt key-id - receive-key-id` - Creates a TCP-AO MKT in the BGP instance.
- `address-family` - Enters the router into the address-family router configuration mode.

- **`show ip bgp - tcp-ao neighbor`** - Displays the TCP-AO information for the specified BGP peer.

31.97 neighbor - tcp-ao mkt

Command Objective This command associates a TCP-AO MKT to the BGP peer.

The no form of the command dissociates a TCP-AO MKT to the BGP peer.

Syntax

```
neighbor <ip-address> tcp-ao mkt <Key Id(0-255)>
no neighbor <ip-address> tcp-ao mkt <Key Id(0-255)>
```

Parameter Description

- `<ip-address>` - Configures the BGP peer for which the TCP-AO MKT configurations are done.
- `<Key Id(0-255)>` -. Configures the Key ID of the MKT which needs to be associated with the peer.. This value ranges between 0 and 255.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

---

☞ This command executes only if BGP Speaker Local AS number and peer is configured.

Example

```
Your Product(config-router)# neighbor 20.45.0.1 tcp-ao mkt
2
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `tcp-ao mkt key-id - receive-key-id` - Creates a TCP-AO MKT in the BGP instance.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp - tcp-ao neighbor` - Displays the BGP(v4) neighbor tcp-ao related information.
- `show ip bgp - tcp-ao mkt summary` - Displays the BGPrelated TCP-AO MKT information.

31.98 neighbor - tcp-ao mkt - start-accept

Command Objective This command configures the time the router will start accepting packets that have been created with the MKT specified by the key-id.

This command is currently not supported.

Syntax `neighbor <ip-address> tcp-ao mkt <Key Id(0-255)> start-accept <DD-MON-YEAR,HH:MM>`

Parameter Description

- `<ip-address>` - Configures the BGP peer for which the TCP-AO MKT configurations are done.
- `<Key Id(0-255)>` -. Configures the Key ID of the MKT which needs to be associated with the peer. This value ranges between 0 and 255.
- `<DD-MON-YEAR,HH:MM>` - Configures the date and time the router will start accepting packets that have been created with the MKT specified by the key-id. For the router to start accepting packets by 10am on 10 January 2012 the input is given as 10-Jan-2012,10:00

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 0000000000000000

This command executes only if BGP Speaker Local AS number and peer is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 tcp-ao mkt 2 start-accept 10-Jun-2013,10:00
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `show ip bgp peer-group` - Displays information about the peer group.
- `address-family` - Enters the router into the address-family router configuration mode.

- `show ip bgp neighbor` – Displays neighbor related information for the peer.

31.99 neighbor - tcp-ao mkt - stop-accept

Command Objective This command configures the time the router will stop accepting packets that have been created with the MKT specified by the key-id.

This command is currently not supported.

Syntax `neighbor <ip-address> tcp-ao mkt <Key Id(0-255)> stop-accept <DD-MON-YEAR,HH:MM>`

Parameter Description

- `<ip-address>` - Configures the BGP peer for which the TCP-AO MKT configurations are done.
- `<Key Id(0-255)>` -. Configures the Key ID of the MKT which needs to be associated with the peer. This value ranges between 0 and 255.
- `<DD-MON-YEAR,HH:MM>` – The date & time the router will stop accepting packets that have been created with the MKT specified by the key-id. For the router to stop accepting packets by 10am on 10 January 2012 the input is given as 10-Jan-2012,10:00.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 0000000000000000

This command executes only if BGP Speaker Local AS number and peer is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 tcp-ao mkt
2 start-accept 10-Jun-2013,10:00
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `show ip bgp peer-group` - Displays information about the peer group.
- `address-family` - Enters the router into the address-family router configuration mode.

- `show ip bgp neighbor` – Displays neighbor related information for the peer.

31.100 neighbor - tcp-ao mkt - start-generate

Command Objective This command configures the time the router will start generating packets that have been created with the MKT specified by the key-id.

This command is currently not supported.

Syntax

```
neighbor <ip-address> tcp-ao mkt <Key Id(0-255)> start-generate <DD-MON-YEAR,HH:MM>
```

Parameter Description

- `<ip-address>` - Configures the BGP peer for which the TCP-AO MKT configurations are done.
- `<Key Id(0-255)>` -. Configures the Key ID of the MKT which needs to be associated with the peer. This value ranges between 0 and 255.
- `<DD-MON-YEAR,HH:MM>` - Configures the date and time the router will start using the MKT specified by the key-id for packets generation. For the router to start generating packets by 10am on 10 January 2012 the input is given as 10-Jan-2012,10:00.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 0000000000000000

This command executes only if BGP Speaker Local AS number and peer is configured.

Example

```
our Product(config-router)# neighbor 23.45.0.1 tcp-ao mkt 1 start-generate 10-Jan-2012,10:10
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `show ip bgp peer-group` - Displays information about the peer group.
- `address-family` - Enters the router into the address-family router configuration mode.

- **`show ip bgp neighbor`** – Displays neighbor related information for the peer.

31.101 neighbor - tcp-ao mkt - stop-generate

Command Objective This command configures the time the router will stop generating packets that have been created with the MKT specified by the key-id.

This command is currently not supported.

Syntax

```
neighbor <ip-address> tcp-ao mkt <Key Id(0-255)> stop-generate <DD-MON-YEAR,HH:MM>
```

Parameter Description

- `<ip-address>` - Configures the BGP peer for which the TCP-AO MKT configurations are done.
- `<Key Id(0-255)>` -. Configures the Key ID of the MKT which needs to be associated with the peer. This value ranges between 0 and 255.
- `<DD-MON-YEAR,HH:MM>` - Configures the date and time the router will stop using the MKT specified by the key-id for packets generation. For the router to stop generating packets by 10am on 10 January 2012 the input is given as 10-Jan-2012,10:00.

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default 0000000000000000

This command executes only if BGP Speaker Local AS number and peer is configured.

Example

```
Your Product(config-router)# neighbor 23.45.0.1 tcp-ao mkt 1 stop-generate 10-Jan-2012,10:10
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `show ip bgp peer-group` - Displays information about the peer group.
- `address-family` - Enters the router into the address-family router configuration mode.

- **`show ip bgp neighbor`** – Displays neighbor related information for the peer.

31.102 show ip bgp - tcp-ao neighbor

Command Objective This command displays the BGP neighbor tcp-ao related information.

The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax `show ip bgp [vrf <vrf-name>] tcp-ao neighbor [<random_str>]`

Parameter Description

- `vrf <vrf-name>` - Displays BGP neighbor tcp-ao related information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.
- `<random_str>` - Displays the BGP neighbor tcp-ao configurations for the specified BGP Peer.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp tcp-ao neighbor 23.45.0.1
    TCP-AO authentication neighbor summary
    -------------------------------------
    Context Name : default
    ------------
    Neighbor    : 23.45.0.1
    MKT Assigned     : 2
    ICMP Processing  : Enabled
    No MKT Discard   : Disabled
    MKT In-use  : None
    TCP-AO authentication neighbor summary
    -------------------------------------
    Context Name : vrf1
    ------------
    Neighbor    : 23.45.0.1
```

```
TCP-AO is not enabled for this peer!!
```

Related Command(s)

- `neighbor - tcp-ao` - sets BGP peer TCP-AO configurations.
- `neighbor - remote-as` – Creates a Peer and initiates the connection to the peer.
- `tcp-ao mkt key-id - receive-key-id` - Creates a TCP-AO MKT in the BGP instance.

31.103 show ip bgp - tcp-ao mkt summary

Command Objective This command displays the BGP related TCP-AO MKT information.

The show command displays information for all vrf instances only if the address-family is set for the specified instance.

Syntax `show ip bgp [vrf <vrf-name>] tcp-ao mkt summary`

Parameter Description

- `vrf <vrf-name>` - Displays the BGP related TCP-AO MKT information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip bgp tcp-ao mkt summary
TCP-AO MKT Table
----------------
Context Name : default
------------
ID(send)  Receive ID  Algorithm  MasterKey  OptionsExclude  Status
--------  ----------  ---------  ---------  --------------  ------
0           1          HMAC-SHA-1  *******     1            Active
255         255        HMAC-SHA-1  *******     1            Active
TCP-AO MKT Table
-----------------
Context Name : vrf1
------------
ID(send)  Receive ID  Algorithm  MasterKey  OptionsExclude   Status
--------  ----------  ---------  ---------  --------------   ------
0           1          HMAC-SHA-1  *******     1            Active
```

Related Command(s)

- `neighbor - tcp-ao mkt` - Associates a TCP-AO MKT to the BGP peer.
- `tcp-ao mkt key-id - receive-key-id` - Creates a TCP-AO MKT in the BGP instance.

31.104 ip bgp four-byte-asn

Command Objective This command enables 4-byte ASN support in BGP speaker or in the specified vrf instance created in the system. This value is a string with maximum size as 32.

When VRF is not specified the configurations are done for the default VRF.

The no form of the command disables 4-byte ASN support in BGP or the specified vrf instance created in the system.

Syntax

```
ip bgp four-byte-asn [vrf <vrf-name>]
no ip bgp four-byte-asn [vrf <vrf-name>]
```

Parameter Description

- `vrf <vrf-name>` - Displays the BGP related TCP-AO MKT information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string with maximum size as 32.

Mode Global Configuration Mode

Default enabled

This command executes only when BGP Speaker Global Admin status is shutdown in the system or the specified vrf insatnce.

Example

```
Your Product(config)# ip bgp four-byte-asn
```

Related Command(s)

- `router-id` - Sets the router ID's address for the router.
- `bgp router-id` – Configures the BGP Identifier of the BGP Speaker.
- `show ip bgp` – Displays the BGP related information.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

31.105 bgp asnotation dot

Command Objective This command changes the output format of BGP ASNs from asplain to asdot notation.

The no form of the command resets the output format of BGP ASNs from asdot to asplain notation.

Syntax

```
bgp asnotation dot
no bgp asnotation dot
```

Mode BGP Router Configuration Mode / Address Family Router Configuration Mode

Default By default, the output format of BGP ASNs is asplain

☞ BGP asnotation can be changed only if four-byte-asn is enabled.

Example

```
Your Product(config-router)# bgp asnotation dot
```

Related Command(s)

- `router bgp` – Sets the AS number of the BGP Speaker.
- `address-family` - Enters the router into the address-family router configuration mode.
- `show ip bgp info` – Displays the BGP related information.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.
- `show ip bgp neighbor` – Displays neighbor related information for the peer.

32 Loop Protect

The Loop protection provides protection against loops by transmitting Configuration-Test-Protocol packets out of ports on which loop protection has been enabled. When the switch sends out a loop protocol packet and then receives the same packet on a port, it will block the port between transmitted port and received port which has disadvantaged

The scope of Loop protect is limited to the configuration of Loop Protection features and related changes on other switch features for supporting Loop Protection.

Spanning-Tree Protocol (STP) in the system plays the similar role with loop protection. Under the physical interface, STP and loop protect should be enabled only one of them.

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

- loop-protect enable
- loop-protect disable
- loop-protect disable-period
- loop-protect transmit-interval
- loop-protect
- show loop-protect

32.1 loop-protect enable

Command Objective This command configures the loop-protect enable. The loop-protect enable is a global configuration. By default, is disabled. Choose Enable to enable loop protection feature.

Syntax `loop-protect enable`

Parameter Description

- `enable` - Enable loop protection feature.

Mode Global Configuration Mode

Default disable

Example

```
Your Product(config)# loop-protect enable
```

Related Command(s)

- `loop-protect disable-period` - loop protection disable period in seconds for ports causing loop sets the IP address for an interface
- `loop-protect transmit-interval` -loop protection transmit interval in seconds
- `loop-protect disable` – Disable loop protection feature
- `show loop-protect` – Display loop protect configuration and status

32.2 loop-protect disable

Command Objective This command configures the loop-protect disable. The loop-protect disable is a global configuration. The default setting is disabled. Choose Enable to enable the loop protection feature.

Syntax `loop-protect disable`

Parameter Description

- `disable` - Disable the loop protection feature.

Mode Global Configuration Mode

Default disable

Example

```
Your Product(config)# loop-protect disable
```

Related Command(s)

- `loop-protect disable-period` - loop protection disable period in seconds for ports causing loop sets the IP address for an interface
- `loop-protect transmit-interval` -loop protection transmit interval in seconds
- `loop-protect enable` – Enable loop protection feature
- `show loop-protect` – Display loop protect configuration and status

32.3 loop-protect disable-period

Command Objective This command configures the disabled period in seconds for port causing loop. The following Relation should be observed.

Disable Period >= 3*Transmit Interval

The no form of the command configures the loop protect disabled period to its default value.

Syntax

```
loop-protect disable-period <integer(30-604800)>
no loop-protect disable-period
```

Parameter Description

- `disable-period <integer(30-604800)>` - Configures the parameters for the specified disable period. This value is a string with maximum size as 604800.

Mode Global Configuration Mode

Default

- Disable-Period - 30 seconds

Example

```
Your Product(config)# loop-protect disable-period 30
```

Related Command(s)

- `loop-protect transmit-interval` -loop protection transmit interval in seconds
- `loop-protect enable` – Enable loop protection feature
- `show loop-protect` – Dispaly loop protect configuration and status

32.4 loop-protect transmit-interval

Command Objective This command configures the transmit interval in seconds.

The following Relation should be observed.

Disable Period >= 3*Transmit Interval

The no form of the command configures the loop protect transmit interval to its default value.

Syntax

```
loop-protect transmit-interval <integer(10-30)>
no loop-protect transmit-interval
```

Parameter Description

- `transmit-interval <integer(10-30)>` - Configures the parameters for the specified transmit inverval. This value is a string with maximum size as 30.

Mode Global Configuration Mode

Default Transmit Inverval - 10 seconds

Example

```
Your Product(config)# loop-protect transmit-interval 10
```

Related Command(s)

- `loop-protect disable-period` - loop protection disable period in seconds for ports causing loop
- `loop-protect enable` – Enable loop protection feature
- `show loop-protect` – Display loop protect configuration and status\

32.5 loop-protect

Command Objective This command configures the loop protect test frame format. The number specified by the loop-detection vid command. The switch will send out a loop test frame with specific tag vid. If the command without specific parameter, the switch will send out a un-tag loop test frame.

The no form of the command configures the loop protect test frame. It will remove specific test frame.

Syntax

```
loop-protect [ vid <string> ]
no loop-protect [ vid <string> ]
```

Parameter Description

- `vid <string>` - Configures the parameters for the specified loop protect test frame.

Mode Interface Configuration Mode (Physical Interface Mode)

Default no loop-protect

Example

```
Your Product(config-if)# loop-protect vid 1-10,20
```

Related Command(s)

- `loop-protect disable-period` - loop protection disable period in seconds for ports causing loop
- `loop-protect transmit-interval` -loop protection transmit interval in seconds
- `loop-protect disable` – Disable loop protection feature
- `show loop-protect` – Dispaly loop protect configuration and status

32.6 show loop-protect

Command Objective This command displays loop protect related information available in the switch for the current loop protect enabled in the switch.

The information contain status, transmit interval, disable period and loop-detectd vid.

Syntax `show loop-protect`

Mode Interface Configuration Mode (Physical Interface Mode)

Example

```
Your Product# show loop-protect
   Loop Protection      : Disabled
   Transmit Interval    : 10 seconds
   Disable Period       : 30 seconds
   Loop Protection Configured Interfaces
   Interface    Status   Loop-Detected( VLAN ID )
   ---------    ------   --------------------------------
   Ex0/1        Up       No
```

Related Command(s)

- `loop-protect disable-period` - loop protection disable period in seconds for ports causing loop
- `loop-protect transmit-interval` -loop protection transmit interval in seconds
- `loop-protect enable` – Enable loop protection feature
- `loop-protect disable` – Disable loop protection feature

33 IPv6

IPv6 is a new version of IP which is designed to be an evolutionary step from IPv4. (Internet Protocol Version 6 is abbreviated to IPv6 (where the “6” refers to the assigned version number 6). The previous version of the Internet Protocol is version 4 (referred to as IPv4)

IPv6 can be installed as a normal software upgrade in Internet devices and is interoperable with the current IPv4. It has expanded routing and addressing capabilities because of the 128 bit addressing as compared to the 32 bit addressing in IPv4. Its deployment strategy is designed to not have any flag days or other dependencies. IPv6 is designed to run well on high performance networks (e.g. Gigabit Ethernet, OC-12, ATM, etc.) and at the same time still be efficient for low bandwidth networks (e.g. wireless). In addition, it provides a platform for new Internet functionality that will be required in the near future.

IPv6 includes a transition mechanism, which is designed to allow users to adopt and deploy IPv6 in a highly diffuse fashion and to provide direct interoperability between IPv4 and IPv6 hosts. The IPv6 transition allows the users to upgrade their hosts to IPv6, and the network operators to deploy IPv6 in routers, with very little coordination between the two.

The changes from IPv4 to IPv6 fall primarily into the following categories

- Expanded Routing and Addressing Capabilities
- Usage of anycast address
- Header Format Simplification
- Improved Support for Options
- Quality-of-Service Capabilities
- Authentication and Privacy Capabilities

The list of CLI commands for the configuration of IPv6 is as follows:

- ipv6 enable
- iipv6 unicast-routing
- ipv6 address - prefix and prefix length
- ipv6 address – ipv6prefix/prefix_length
- ipv6 - static routes
- ipv6 - neighbor
- ipv6 default – hop limit
- ipv6 nd suppress-ra
- ipv6 nd managed-config flag
- ipv6 nd other-config flag
- ipv6 hop-limit
- ipv6 nd ra-lifetime
- ipv6 nd dad attempts

- ipv6 nd reachable-time
- ipv6 nd ns - interval
- ipv6 nd ra mtu
- ipv6 nd ra-interval
- ipv6 nd prefix
- ping ipv6
- debug ipv6
- traceroute6
- clear ipv6 neighbors
- clear ipv6 traffic
- clear ipv6 route
- show ipv6 interface
- show ipv6 route
- show ipv6 route - summary
- show ipv6 neighbors
- show ipv6 neighbors
- ipv6 path mtu discover
- ipv6 path mtu
- show ipv6 pmtu
- ipv6 interface-identifier
- ipv6 icmp error-interval
- ipv6 icmp dest-unreachable
- ipv6 policy-prefix
- ipv6 policy-prefix
- ipv6 unicast-routing – interface configuration
- ipv6 default scope-zone
- ipv6 scope-zone
- show ipv6 addr-sel-policy-table
- show ipv6 scope-zone interface
- show ipv6 zone - if-list
- show ipv6 default scope-zone

33.1 ipv6 enable

Command Objective This command enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.

The no form of the command disables IPv6 processing on the interface.

Syntax

```
ipv6 enable

no ipv6 enable
```

Mode Interface Configuration Mode (VLAN)

Default Disabled

Example

```
Your Product(config)# ipv6 enable
```

Related Command(s)

- `ipv6 address` - prefix and prefix length - Configures IPv6 address on the interface.
- `show ipv6 interface` - Displays the IPv6 interfaces.
- `ipv6 router rip / ipv6 router rip – name` - Enables RIP6 and enters into the router configuration Mode.

33.2 ipv6 unicast-routing

Command Objective This command enables unicast routing which is used for one to one communication across the ipv6 internet. An IPv6 unicast address is an identifier for a single interface, on a single node. A packet that is sent to a unicast address is delivered to the interface identified by that address.

The no form of the command disables unicast routing.

Syntax

```
ipv6 unicast-routing [vrf <vrf-name>]

no ipv6 unicast-routing [vrf <vrf-name>]
```

Parameter Description

- `vrf <vrf-name>` - Configures ipv6 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 Enabled

Example

```
Your Product(config)# ipv6 unicast-routing
```

Related Command(s)

- `ipv6 router rip / ipv6 router rip – name` - Enables RIP6 and enters into the router configuration Mode.
- `ip vrf`– Create VRF instance.

33.3 ipv6 address - prefix and prefix length

Command Objective This command configures IPv6 address on the interface.

The no form of the command deletes the configured IPv6 address.

Syntax

```
ipv6 address <prefix> <prefix Len> [{unicast | anycast | eui64}]
```

```
no ipv6 address <prefix> <prefix Len> [{unicast | anycast | eui64}]
```

Parameter Description

- `<prefix>` - Configures the IPv6 prefix for the interface.
- `<prefix Len>` - Configures the number of high-order bits in the IPv6 address. These bits are common among all hosts within a network. This value ranges between 0 and 128.
- `unicast` - Configures the address type of the prefix as Unicast.
- `anycast` - Configures the address type of the prefix as Anycast.
- `eui64` - Configures the type of Prefix where the latter 64 bits are formed from the link layer address.

Mode Interface Configuration Mode (VLAN)

Default unicast

☞ The prefix length for eui64 type must be 64

Example

```
Your Product(config-if)# ipv6 address 3333::1111 64 unicast
```

Related Command(s)

- `show ipv6 interface` –Displays the IPv6 interfaces.

33.4 ipv6 address - ipv6prefix/prefix_length

Command Objective This command configures IPv6 address on the interface.

This command is a standardized implementation of the existing command; ipv6 address - prefix and prefix length. It operates similar to the existing command.

Syntax `ipv6 address <ipv6prefix/prefix_length> [{unicast | anycast | eui-64| link-local}]`

Parameter Description

- `<ipv6prefix>` - Configures the IPv6 prefix for the interface.
- `<prefix_length>` - Configures the number of high-order bits in the IPv6 address. These bits are common among all hosts within a network. This value ranges between 0 and 128.
- `unicast` - Configures the address type of the prefix as Unicast.
- `anycast` - Configures the address type of the prefix as Anycast.
- `eui64` - Configures the type of Prefix where the latter 64 bits are formed from the link layer address.
- `link-local` - Configures the Link local type prefix.

Mode Interface Configuration Mode (VLAN)

Default unicast

☞ The prefix length for eui64 type must be 64

Example

```
Your Product(config-if)# ipv6 address 3333::1111/64 unicast
```

Related Command(s)

- show ipv6 interface –Displays the IPv6 interfaces.

33.5 ipv6 address - link local

Command Objective This command configures the IPv6 link-local address on the interface. The link-local address is an IP address that is intended only for communications within the segment of a local network (a link) or a point-to-point connection.

The no form of the command deletes the configured IPv6 link-local address.

Syntax

```
ipv6 address <prefix> link-local
no ipv6 address <prefix> link-local
```

Parameter Description

- `<Prefix>` - Configures the IPv6 prefix for the interface.

Mode Interface Configuration Mode (VLAN)

Default fe80::204:2ff:fe03:401 [Down] [scope:Linklocal]

☞ The prefix length for eui64 type must be 64

Example

```
Your Product(config-if)# ipv6 address fe80::2222 link-local
```

Related Command(s)

- `show ipv6 interface` – Displays the IPv6 interfaces.

33.6 ipv6 - static routes

Command Objective This command configures static routes which are manually configured and define an explicit path between two networking devices. The static routes are not automatically updated and must be manually reconfigured if the network topology changes.

The no form of the command deletes the configured static routes.

Syntax

```
ipv6 route [vrf <vrf-name>] <prefix> <prefix len>
[<NextHop>] [{vlan <vlan-id/ vfi-id> [switch <switch-name>]
[<administrative distance>] [{unicast | anycast}] | tunnel
<id> [<administrative distance>] [unicast] |
[<administrative distance>] [unicast] | <interface-type>
<interface-id> [<administrative distance>] [unica st] |
<IP-interface-type> <IP-interface-number> [<administrative
distance>] [unicast]}]
```

```
no ipv6 route [vrf <vrf-name>] <prefix> <prefix len>
[<NextHop>] [{vlan <vlan- id/vfi-id> [switch <switch-name>]
| tunnel <id> [<administrative distance>] [uni cast] |
<interface-type> <interface-id> [<administrative distance>]
[unicast] | <IP-interface-type> <IP-interface-number>
[<administrative distance>] [unicast]}
```

Parameter Description

- `vrf <vrf-name>` - Configures ipv6 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 IPv6 Prefix of the destination.
- `<prefix len>` - Configures the number of high-order bits in the IPv6 address. These bits are common among all hosts within a network. This value ranges between 0 and 128.
- `<Next-Hop>` - Configures the IPv6 prefix of the next hop that is used to reach the destination network.
- `vlan <vlan-id/vfi-id>` - Configures IPv6 static routes 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.

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 ipv6 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.
  - **administrative distance** - Configures the metric to reach the destination. The value ranges between 0 and 65535.
  - **unicast** - Configures the prefix type as Unicast.
  - **anycast** - Configures the prefix type as Anycast.
- **tunnel<id>** - Configures the Tunnel Identifier.
  - **administrative distance** - Configures the metric to reach the destination. The value ranges between 0 and 65535.
  - **unicast** - Configures the unicast type of prefix.
- **<interface-type>** - Configures static routes 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.
- **<interface-id>** - Configures static routes 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 i-lan ID is provided, for interface types i-lan. For example: 1 represents i-lan ID.
  - **administrative distance** - Configures the metric to reach the destination. The value ranges between 0 and 65535.

- `unicast` - Configures the unicast type of prefix.

- `<IP-interface-type>` - Configures static routes in the specified L3 Psuedo wire interface in the system.
- `<IP-interface-number>` - Configures static routes 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.

  – `administrative distance` - Configures the metric to reach the destination. The value ranges between 0 and 65535.
  – `unicast` - Configures the unicast type of prefix.

Mode Global Configuration Mode

Default

- administrative distance - 1
- vrf - default
- unicast

- A Route will be configured only when a proper route exists for the next-hop prefix in the route table. Also the duplicate address detection should be completed and the address should not be in tentative state.
- VRF instance should be created, before executing this command to configure the static routes for the context.
- VRF instance should be mapped to the IPV4 / IPV6 interface, before executing this command to configure the static routes for the context in the interface.

Example

```
Your Product(config)# ipv6 route 1111::2872 7 vlan 1
switch default 99903 anycast
```

Related Command(s)

- `ipv6 – link local address` –Configures the IPv6 link-local address on the interface.
- `show ipv6 route` –Displays the IPv6 Routes.
- `ip vrf` –Creates VRF instance.

- `ip vrf forwarding` –Creates VRF instance.

33.7 ipv6 neighbor

Command Objective This command configures a static entry in the IPv6 neighbor cache table.

The no form of the command removes the static entry from the IPv6 neighbor cache table.

Syntax

```
ipv6 neighbor [vrf <vrf-name>] <prefix> {vlan <vlan-id/vfi-id> [switch <switch-name>] | tunnel <id> | <IP-interface-type> <IP-interface-number>  | mgmt } <MAC ADDRESS (xx:xx:xx:xx:xx:xx)>
```

```
no ipv6 neighbor [vrf <vrf-name>] <prefix> {vlan <vlan-id/vfi-id> [switch <switch-name>] | tunnel <id> | <IP-interface-type> <IP-interface-number> | mgmt }
```

Parameter Description

- `vrf <vrf-name>` - Configures ipv6 for the specified VRF instance. This value is a string whose maximum size is 32.
- `<prefix>` - Configures the IPv6 Prefix of the neighbor.
- `vlan <vlan-id/vfi-id>` - Configures a static entry in the IPv6 neighbor cache table 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.

    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 ipv6 for the specified context representing a unique name of the switch context. This value is a string whose maximum size is 32and is specific to multiple instance feature.
- **tunnel<id>** - Configures the Tunnel Identifier. ID range varies between 0 and 128.
- **<IP-interface-type>** - Configures static entry in the IPv6 neighbor cache table for the specified L3 Psuedo wire interface in the system.
- **<IP-interface-number>** - Configures static entry in the IPv6 neighbor cache table 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.
- **mgmt** - Configures static entry in the IPv6 neighbor specified L3 cache table for management interface.
- **<MAC ADDRESS(xx:xx:xx:xx:xx:xx)>** - Configures the Link layer address of the interface address range.

Mode Global Configuration Mode

- VRF instance should be created, before executing this command to configure the static entry for the context.
- VRF instance should be mapped to the IPV4 / IPV6 interface, before executing this command to configure the static entry for the context in the interface.
- Tunnel ID should be created before executing the command

Example

```
Your Product(config)# ipv6 neighbor 3333::1111 vlan 1
00:11:22:33:44:55
```

Related Command(s)

- **clear ipv6 neighbors** –Removes all the entries in the IPv6 neighbor table.
- **show ipv6 neighbors** –Displays the IPv6 Neighbor Cache Entries.
- **ip vrf** –Creates VRF instance.
- **ip vrf forwarding** –Maps the IPV4 / IPV6 interface to the
- context.
- **int tunnel** –Creates Tunnel ID.

33.8 ipv6 default – hop limit

Command Objective This command sets the default hop limit for IPv6 Datagrams, where the Hop Limit value should place in the router advertisements sent on the IPv6 interface.

The no form of command resets default hop limit for IPv6 Datagrams

---

Syntax

```
ipv6 default-hop limit [vrf <vrf-name>] <HopLimit (1-255)>

no ipv6 default-hop limit [vrf <vrf-name>]
```

Parameter Description

- `vrf <vrf-name>` - Configures ipv6 for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
- `<HopLimit (1-255)>` - Configures the hop limit value for the ipv6 datagrams. The value ranges between 1 to 255

Mode Global Configuration Mode

☞

- VRF instance should be created, before executing this command to configure the default hop limit for the context.

Example

```
Your Product(config)# ipv6 default-hop limit 100
```

Related Command(s)

- `ip vrf` – Creates VRF instance.

33.9 ipv6 nd suppress-ra

Command Objective This command suppresses IPv6 router advertisement.

The no form of the command enables IPv6 router advertisement.

Syntax	`ipv6 nd suppress-ra` `no ipv6 nd suppress-ra`
Mode	Intrfac Configuration Mode (VLAN)
Default	Router advertisements are suppressed
Example	`Your Product(config-if)# ipv6 nd suppress-ra`

Related Command(s)

- `show ipv6` – Displays the IPv6 interfaces.
- `show ipv6 traffic` – Displays the IPv6 ICMP and UDP statistics.

33.10 ipv6 nd managed-config flag

Command Objective This command sets the 'Managed config flag' which allows the host to use DHCP for address configuration. This Flag is used to enable or disable Path MTU Discovery for the node.

The no form of the command resets the 'Managed config flag' which does not allow the host to use DHCP for address configuration.

Syntax

```
ipv6 nd managed-config flag
```

```
no ipv6 nd managed-config flag
```

Mode Interface Configuration Mode (VLAN)

Default Global

Example

```
Your Product(config-if)# ipv6 nd managed-config flag
```

33.11 ipv6 nd other-config flag

Command Objective This command sets the 'other config flag' which allows the host to use DHCP for other stateful configuration.

The no form of the command resets the 'other config flag'

Syntax

```
ipv6 nd other-config flag

no ipv6 nd other-config flag
```

Mode Interface Configuration Mode (VLAN)

Default Global

Example

```
Your Product(config-if)# ipv6 nd other-config flag
```

Related Command(s)

- `no ip v6 nd suppress-ra` – Enables IPv6 router advertisement

33.12 ipv6 hop-limit

Command Objective This command configures the maximum hoplimit for all IPv6 packets originating from the interface. The hop limit value ranges between 0 and 255.

The hop limit value ranges between 1 and 255 if the unicast routing is disabled on the interface.

The no form of the command resets the hoplimit to default value for all IPv6 packets

---

Syntax

```
ipv6 hop-limit <HopLimit (0-255)>

no ipv6 hop-limit
```

Mode Interface Configuration Mode (VLAN)

Default 64

Example

```
Your Product(config-if)# ipv hop-limit 100
```

Related Command(s)

- `ipv6 unicast-routing` - Enables unicast routing on the interface. interface.

33.13 ipv6 nd ra-lifetime

Command Objective This command sets the IPv6 Router Advertisement lifetime and specifies the preferred lifetime in seconds for the address prefixes corresponding to those addresses which use this profile. The value of the lifetime ranges between 0 and 9000

Syntax `ipv6 nd ra-lifetime <LifeTime (0-9000)>`

Mode Interface Configuration Mode

Default 1800 seconds

☞ The ND RA lifetime value must be greater than or equal to the RA interval.

Example

```
Your Product(config-if)# ipv6 nd ra-lifetime 100
```

Related Command(s)

- `no ip v6 nd suppress-ra` –Enables IPv6 router advertisement.
- `show ipv6 interface` –Displays the IPv6 interfaces.

33.14 ipv6 nd dad attempts

Command Objective This command sets the number of duplicate address detection (dad) attempts, where the maximum number of neighbor solicitations sent for the purpose of duplicate address detection on a tentative address. The value of the number of duplicate address detection attempt ranges between 0 and 10.

The no form of the command resets the duplicate address detection attempts to its default value.

Syntax

```
ipv6 nd dad attempts <no of attempts (1-10)>

no ipv6 nd dad attempts
```

Mode Interfac Configuration Mode (VLAN)

Default 1

Example

```
Your Product(config-if)# ipv6 nd dad attempts 5
```

Related Command(s)

- `show ipv6 interface` – Displays the IPv6 interfaces.
- `no ip v6 nd suppress-ra` – Enables IPv6 router advertisement.

33.15 ipv6 nd reachable-time

Command Objective This command sets the advertised reachability time which is to be indicated in the router advertisements sent on this IPv6 interface and is also used by this entity.

The no form of the command resets the advertised reachability time to default value.

Syntax

```
ipv6 nd reachable-time {<Reachable Time (0-3600)> | msec
<Reachable Time (0-3600000)> }

no ipv6 nd reachable-time
```

Parameter Description

- `<Reachable Time (0-3600)>` - Defines the time in seconds that a neighboring node is considered to be reachable after having received the reachability confirmation from that node. This value ranges between 0 and 3600.
- `msec <Reachable Time (0-3600000)>` - Defines the time in milli seconds that a neighboring node is considered to be reachable after having received the reachability confirmation from that node. This value ranges between 0 and 3600 in milliseconds.

Mode Interface Configuration Mode (VLAN)

Default 30

Example

```
Your Product(config-if)# ipv6 nd reachable-time 500
```

Related Command(s)

- `show ipv6 interface` –Displays the IPv6 interfaces.
- `no ip v6 nd suppress-ra` –Enables IPv6 router advertisement.

33.16 ipv6 nd ns - interval

Command Objective This command sets the advertised retransmission time which is to be indicated in the router advertisements sent on this IPv6 interface and also used by this entity. Defines the time in milli seconds between retransmitted Neighbor Solicitations which is used during address resolution, unreachability detection and duplicate address detection. This value ranges between 1000 and 3600000 in milliseconds.

The no form of the command resets the advertised retransmission time to default value.

Syntax

```
ipv6 nd ns-interval <Retranmission time (1000-3600000) in milliseconds>

no ipv6 nd ns-interval
```

Mode Interface Configuration Mode

Default Global

Example

```
Your Product(config-if)# ipv6 nd ns-interval 1000
```

Related Command(s)

- `show ipv6 interface` –Displays the IPv6 interfaces.

33.17 ipv6 nd ra mtu

Command Objective This command sets router advertisement MTU optional value which contains an entry for a specific path traversed by packets exchanged between the source and destination nodes.. The value ranges between 1280 and 1500.

The no form of the command resets router advertisement MTU option value to its default value.

Syntax

```
ipv6 nd ra-mtu <router advertisement MTU option vlaue(1280-1500)>

no ipv6 nd ra-mtu
```

Mode Interface Configuration Mode (VLAN)

Default 1500

Example

```
Your Product(config-if)# ipv6 nd ra-mtu 1400
```

Related Command(s)

- `show ipv6 interface` –Displays the IPv6 interfaces.

33.18 ipv6 nd ra-interval

Command Objective This command sets the IPv6 Router Advertisement interval.

The no form of the command resets the IPv6 Router Advertisement interval to its default value.

Syntax

```
ipv6 nd ra-interval <maximum-interval-secs(4-1800)>
[<minimum-interval-secs(3-1350)>]

no ipv6 nd ra-interval
```

Parameter Description

- `<maximum interval-secs (4-1800)>` - Configures the maximum time in seconds between sending unsolicited router advertisements. Router advertisements are sent periodically at a random interval between the values 4 to 1800. Maximum interval should be greater than or equal to 4/3 times of the minimum interval.
- `<minimum-interval-secs(3-1350)>` - Configures the minimum time in seconds allowed between sending unsolicited router advertisements. The default value is one-third the default value of router advertisement time. The value can be configured in the range between 3 seconds and 1350.

Mode Interface Configuration Mode (VLAN)

Default

- Maximum interval – 600 seconds
- Minimum interval – 198 seconds

Example

```
Your Product(config-if)# ipv6 nd ra-interval 20
```

Related Command(s)

- `show ipv6 interface` –Displays the IPv6 interfaces.
- `no ip v6 nd suppress-ra` –Enables IPv6 router advertisement.

33.19 ipv6 nd prefix

Command Objective This command configures the prefix to be advertised in IPv6 Router Advertisement.

The no form of the command removes the prefix from the IPv6 Router Advertisement.

Syntax

```
ipv6 nd prefix {<prefix addr> <prefixlen> | default}
[{{<valid lifetime> | infinite | at <var valid
lifetime>}{<preferred lifetime> |infinite | at <var
preferred lifetime>} | no-advertise}] [off-link] [no-
autoconfig] [embedded-rp]

no ipv6 nd prefix {<prefix addr> <prefix len> | default}
```

Parameter Description

- `<prefix addr>` - Configures the IPv6 prefix which is to be advertised
- `<prefixlen>` - Configures the number of high-order bits in the IPv6 address. These bits are common among all hosts within a network. This value range between 1 and 128.
- `default` - Changes the default value of the rest of the parameters.
- `<valid lifetime>` - Sets the valid lifetime value for the prefix in seconds for the address prefixes corresponding to those addresses which use this profile. This is sent in router advertisements by this entity. This value ranges between 0 and 4294967295.
- `infinite` - Sets the infinite valid lifetime value for the prefix
- `at <var valid lifetime>` - Sets the variab le valid lifetime value for the prefix. This value ranges between 0 and 4294967295.
- `<preferred lifetime>` - Sets the preferred lifetime value for the prefix in seconds for the address prefixes corresponding to those addresses which use this profile. This is sent in router advertisements by this entity. This value ranges between 0 and 4294967295.
- `infinite` - Sets the infinite Preferred lifetime value for the prefix.
- `at<var preferred lifetime>` - Sets the variable valid lifetime value for the prefix. This value ranges between 0 and 4294967295.
- `no-advertise` - Sets the No-Advertise flag for the prefix.
- `off-link` - Sets the off-link flag for the prefix.
- `no-autoconfig` - Sets the no-autoconfig flag for the prefix.
- `embedded-rp` - Sets the embedded rp.

Mode Interface Configuration Mode (VLAN)

Default

- ra valid lifetime – 25,9200 seconds
- ra preferred lifetime – 60,4800 seconds

☞ Valid life-time must be greater than or equal to preferred life-time.

Example

```
Your Product(config-if)# ipv6 nd prefix 3333::1111  64 500
400
```

Related Command(s)

- `show ipv6 interface` –Displays the IPv6 interfaces.

33.20 ping ipv6

Command Objective This command sends IPv6 echo messages along with the total number of packets to the destination.

Syntax

```
ping [vrf <vrf-name>] ipv6 <prefix%interface> [data
<hex_str>] [repeat <count>] [size <value>] [anycast]
[source { vlan <vlan-id/vfi-id>  [switch <switch-name>] |
tunnel <id> | <source_prefix>}  | <interface-type>
<interface-id> ] [timeout <value (1-100)>]
```

Parameter Description

- `vrf <vrf-name>` - Configures ipv6 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%interface>` - Configures the IPv6 Destination Prefix
- `data<hex_str>` - Configures the data which to be sent in ping. message.
- `repeat<count>` - Configures the number of ping messages. The range varies between 0 and 10.
- `size<value>` - Configures the size of the data portion of the Ping packet in the message.
- `anycast` - Configures the Type of Prefix
- `source <vrf-name>` - Configures the Source Interface of the ping message.
- `vlan <vlan-id/vfi-id>` - Sends IPv6 echo messages 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

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 ipv6 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.
- **tunnel <id>** - Configures tunnel source interface of the ping message. ID range varies between 0 and 128.
- **<source_prefix>** - Configures source prefix of the ping message.
- **<interface-type>** - Configures static routes 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.
- **<interface-id>** - Configures static routes 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.
- **timeout <value (1-100)>** - Configures the time in seconds after which this entity times out waiting for a particular ping response. The value ranges between 1 to 100.

Mode Privileged EXEC Mode

Default

- data – a5a4
- repeat <count> – 5
- size – 100 bytes

- Router port doesn't support the syntax of **<prefix%interface>** when destination is a link local address. Need the specified interface type and number by source option.

- VRF instance should be created, before executing this command to send echo mssags for the context.
- VRF instance should be mapped to the IPV4 / IPV6 interface, before executing this command to send echo messages for the context in the interface.
- Tunnel ID must be created before executing the command.

Example `Your Product# ping ipv6 3333::1111 data a6b6`

Related Command(s)

- `ip vrf` – Creates VRF instance.
- `ip vrf forwarding` – Creates VRF instance.
- `int tunnel` – Creates tunnel ID.

33.21 debug ipv6

Command Objective This command enables IPv6 Trace.

The no form of the command disables IPv6 Trace

Syntax `debug ipv6 [vrf <vrf-name>] {IP6|ICMP|UDP6|ND|PING6|TUNNEL}`

`no debug ipv6 [vrf <vrf-name>]`

Parameter Description

- `vrf <vrf-name>` - Configures ipv6 for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
- `IP6` - Generates debug statements for IP6 Trace.
- `ICMP` - Generates debug statements for ICMP Trace.
- `UDP6` - Generates debug statements for UDP6 Trace.
- `ND` - Generates debug statements for Neighbor Discovery Trace.
- `PING6` - Generates debug statements for PING6 Trace.
- `TUNNEL` - Generates debug statements for Tunnel Trace.

Mode Privileged EXEC Mode

Default Debug traces are disabled

☞ VRF instance should be created, before executing this command to configure IPv6 trace for the context.

Example

```
Your Product# debug ipv6 IP6
```

Related Command(s)

- `ip vrf` –Creates VRF instance.

33.22 traceroute6

Command Objective This command traces route to the destination

Syntax `traceroute6 <ip-address> [vrf <vrf-name>] [min-ttl <value (1-99)>] [max-ttl <value(1-99)>]`

Parameter Description

- `<ip-address>` - Configurest the destination IP address to which a route has to be traced.
- `vrf <vrf-name>` - Configures ipv6 for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
- `min-ttl<value (1-99)>` - Configures the minimum value of the TTL field to be filled up in the IP packets used for the trace route. This value ranges between 1 and 99 seconds.
- `max-ttl<value (1-99)>` - Configures the maximum value of the TTL field to be filled up in the IP packets used for the trace route. This value ranges between 1 and 99 seconds.

Mode Privileged EXEC Mode

Default

- min-ttl – 1
- max-ttl – 15

☞

- VRF instance should be created, before executing this command to trace routes for the context.
- The maximum value of the TTL field should be always greater than the minimum value of the TTL field.

Example

```
Your Product# traceroute6 4444::1111 min-ttl 20 max-ttl 99
```

Related Command(s)

- `ip vrf` –Creates VRF instance.

33.23 clear ipv6 neighbors

Command Objective This command removes all the entries in the IPv6 neighbor table.

Syntax `clear ipv6 neighbors [vrf <vrf-name>]`

Parameter Description

- `vrf <vrf-name>` - Clears ipv6 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

☞ VRF instance should be created, before executing this command to clear neighbor entries for the context.

Example

```
Your Product# clear ipv6 neighbors
```

Related Command(s)

- `ipv6 neighbor` –Configures a static entry in the IPv6 neighbor. cache table..
- `show ipv6 neighbours` –Displays the IPv6 neighbor cache entries.

33.24 clear ipv6 traffic

Command Objective This command removes all the entries in the IPv6 traffic table.

Syntax `clear ipv6 traffic [vrf <vrf-name>]`

Parameter Description

- `vrf <vrf-name>` - Clears entris for the specified VRF instance in the IPv6 traffic table. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Mode Privileged EXEC Mode

☞ VRF instance should be created, before executing this command to clear traffic entries for the context.

Example

```
Your Product# clear ipv6 traffic
```

Related Command(s)

- `show ipv6 traffic` –Displays the IPv6 ICMP and UDP statistics.
- `ip vrf` –Creates VRF instance.

33.25 clear ipv6 route

Command Objective This command removes all the entries in IPv6 route table.

Syntax `clear ipv6 route [vrf <vrf-name>]p`

Parameter Description

- `vrf <vrf-name>` - Clears entry for the specified VRF instance in the IPv6 route table. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.

Mode Privileged EXEC Mode

☞ VRF instance should be created, before executing this command to remove routes for the context.

Example

```
Your Product# clar ipv6 route
```

Related Command(s)

- `show ipv6 route` – Displays the IPv6 Routes.
- `ip vrf` –Creates VRF instance.

33.26 show ipv6 interface

Command Objective This command displays the IPv6 interfaces.

Syntax

```
show ipv6 interface [vrf <vrf-name>] [{vlan <vlan-id/vfi-id> [switch <switch-name>] | tunnel <id>| <interface-type> <if-num> | <ipiftype> <ifnum>} [prefix]]
```

Parameter Description

- `vrf <vrf-name>` - Displays the ipv6 interface details 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 ipv6 interface details 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.

  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 ipv6 interface details 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.
- `tunnel <id>` - Displays the ipv6 interface details for tunnel source interface of the ping message.
- `<interface-type>` - Displays ipv6 information 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.

- **<if-num>** - Displays ipv6 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. For example: 0/1 represents that the slot number is 0 and port number is 1.
- **<ipiftype>** - Displays the IPv6 configuration for the specified L3 Psuedo wire interface in the system.
- **<ifnum>** - Displays IPv6 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.
- **prefix** - Displays the ipv6 interface details for the Prefix information for the ipv6 interface.

Mode Privileged EXEC Mode

Example

```
Your Product#show ipv6 interface
    VRF Id  : 0
    VRF Name: default
    vlan1 is up, line protocol is up
        Forwarding operationally Enabled
        Link local address:
            fe80::ec4:7aff:fe1a:4aea [scope: Linklocal]
        Global unicast address(es):
            Not Configured.
        Joined group address(es):
            ff02::1 Scope:[Multicast linklocal]
            ff02::2 Scope:[Multicast linklocal]
            ff02::1:ff1a:4aea Scope:[Multicast linklocal]
        MTU is 1500
        ICMP redirects are enabled
```

```
        ND DAD is enabled, Number of DAD attempts: 1
        Destination Unreachable error messages enabled
        ICMPv6 Error Rate Limiting Enabled
        ICMPv6 Error Rate-Limit Interval: 100
        ICMPv6 Error Rate-Limit Bucket Size: 10
        ND router advertisement is disabled
        IPv6 current Hop-Limit: 0
    VRF Id  : 1
    VRF Name: mgmt
    mgmt is up, line protocol is up
        Link local address:
            fe80::ec4:7aff:fe1a:4ae8 [scope: Linklocal]
        Global unicast address(es):
            3ffe:100::ec4:7aff:fe1a:4ae8/64 [Scope:GLOBAL]
        Joined group address(es):
            ff02::1 Scope:[Multicast linklocal]
            ff02::1:ff1a:4ae8 Scope:[Multicast linklocal]
        MTU is 1500
        ND DAD is enabled, Number of DAD attempts: 1
        Destination Unreachable error messages enabled
        ICMPv6 Error Rate Limiting Enabled
        ICMPv6 Error Rate-Limit Interval: 100
        ICMPv6 Error Rate-Limit Bucket Size: 10
        IPv6 current Hop-Limit: 64
Your Product#show ipv6 interface vrf vlan 1
    VRF Id  : 0
    VRF Name: default
    vlan1 is up, line protocol is up
        Forwarding operationally Enabled
```

```
Link local address:
    fe80::ec4:7aff:fe1a:4aea [scope: Linklocal]
Global unicast address(es):
    Not Configured.
Joined group address(es):
    ff02::1 Scope:[Multicast linklocal]
    ff02::2 Scope:[Multicast linklocal]
    ff02::1:ff1a:4aea Scope:[Multicast linklocal]
MTU is 1500
ICMP redirects are enabled
ND DAD is enabled, Number of DAD attempts: 1
Destination Unreachable error messages enabled
ICMPv6 Error Rate Limiting Enabled
ICMPv6 Error Rate-Limit Interval: 100
ICMPv6 Error Rate-Limit Bucket Size: 10
ND router advertisement is disabled
IPv6 current Hop-Limit: 0
```

Related Command(s)

- **ipv6 enable** – Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
- **ipv6 address** – prefix and prefix length - / ipv6 address - ipv6prefix/prefix_length – Configures IPv6 address on the interface.
- **ipv6** –link local address – Configures the IPv6 link-local address on the interface.
- **ipv6 nd suppress-ra** – Suppresses IPv6 router advertisement.
- **ipv6 nd ra-lifetime** – Sets the IPv6 Router Advertisement lifetime.
- **ipv6 nd dad attempts** – Sets Duplicate Address Detection attempts.
- **ipv6 nd reachable-time** – Sets the advertised reachability time.
- **ipv6 nd ra-interval** – Sets the IPv6 Router Advertisement interval.
- **ipv6 nd prefix** – Configures the prefix to be advertised in IPv6 Router Advertisement.

33.27 show ipv6 route

Command Objective This command displays the IPv6 Routes.

Syntax `show ipv6 route [vrf <vrf-name>]`

Parameter Description

- `vrf <vrf-name>` - Displays ipv6 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 Model

Example

```
Your Product# show ipv6 route
    VRF Name: default
    ---------------
    IPv6 Routing Table:
    Codes : C - Connected, S - Static
    O - OSPF, R - RIP, B - BGP, I - ISIS
    C 1111::/64 [1/1]
      via ::, vlan 1
    C 2222::/64 [1/1]
      via ::, vlan 2
    VRF Name: mgmt
    ---------------
    IPv6 Routing Table:
    Codes : C - Connected, S - Static
    O - OSPF, R - RIP, B - BGP, I - ISIS
    C 3333::/64 [1/1]
      via ::, mgmt
Your Product# show ipv6 route vrf default
```

```
VRF Name: default

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

IPv6 Routing Table:

Codes : C - Connected, S - Static

O - OSPF, R - RIP, B - BGP, I - ISIS

C 1111::/64 [1/1]

  via ::, vlan 1

C 2222::/64 [1/1]

  via ::, vlan 2
```

Related Command(s)

- `ipv6 - static routes` – Configures static routes

33.28 show ipv6 route - summary

Command Objective This command displays the summary of IPv6 Routes.

Syntax `show ipv6 route [vrf <vrf-name>] summary`

Parameter Description

- `vrf <vrf-name>` - Displays the summary of the ipv6 routes 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 Model

Default Global

Example

```
Your Product# show ipv6 route summary
    VRF Name: default
    ---------------
    IPv6 Routing Table Summary - 2 entries
        2 Connected, 0 Static, 0 RIP, 0 BGP, 0 OSPF
        Number of prefixes:    /64: 2
    VRF Name: mgmt
    ---------------
    IPv6 Routing Table Summary - 3 entries
        1 Connected, 0 Static, 0 RIP, 0 BGP, 0 OSPF
        Number of prefixes:
        /64: 2
Your Product# show ipv6 route vrf default summary
    VRF    Name:      default
    ---------------
    IPv6 Routing Table Summary - 2 entries
        2 Connected, 0 Static, 0 RIP, 0 BGP, 0 OSPF
```

```
Number of prefixes:
/64: 2
```

Related Command(s)

- `ipv6 - static routes` – Configures static routes.

33.29 show ipv6 neighbors

Command Objective This command displays the IPv6 Neighbor Cache Entries.

Syntax `show ipv6 neighbors [vrf <vrf-name>]`

Parameter Description

- `vrf <vrf-name>` - Displays ipv6 information of the neighbors 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 Model

Example

```
Your Product# show ipv6 neighbors
VRF Id  : 0
VRF Name: default
    IPv6 Address    Link-layer Addr     State     Interface
     -----------     ---------------     -----     ---------
3333::1111          00:11:22:33:44:55   Static     vlan2000
1 Neighbor Cache entries.
    REACHABLE : 0
    STALE : 0
    DELAY : 0
    PROBE : 0
    INCOMPLETE : 1
VRF Id  : 1
VRF Name: mgmt
IPv6 Address            Link-layer Addr     State   Interface
fe80::225:90ff:feb2:b03f  00:25:90:b2:b0:3f  Stale   mgmt

1 Neighbor Cache entries.
    REACHABLE : 0
```

```
   STALE : 1
   DELAY : 0
   PROBE : 0
   INCOMPLETE : 0
Your Product# show ipv6 neighbors vrf default
   VRF Id  : 0
   VRF Name: default
       IPv6 Address    Link-layer Addr    State   Interface
       ------------    ---------------     -----   ---------
     3333::1111        00:11:22:33:44:55  Static   vlan2000
   1 Neighbor Cache entries.
       REACHABLE : 1
       STALE : 0
       DELAY : 0
       PROBE : 0
       INCOMPLETE : 0
```

Related Command(s)

- `ipv6 - neighbor` – Configures a static entry in the IPv6 neighbor cache table.
- `clear ipv6 neighbors` – Removes all the entries in the IPv6 neighbor table.

33.30 show ipv6 traffic

Command Objective This command displays the IPv6 ICMP and UDP statistics.

Syntax

```
show ipv6 traffic [vrf <vrf-name>] [interface { vlan
<vlan-id/vfi-id> [switch <switch-name>] | tunnel <tunnel-
id> | <interface-type> <if-num> | <IP-interface-type> <IP-
interface-number>} ] [hc]
```

Parameter Description

- `vrf <vrf-name>` - Displays the IPv6 ICMP and UDP statistics 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 IPv6 ICMP and UDP 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.

    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

    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 IPv6 ICMP and UDP 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.
- `tunnel <id>` - Displays the IPv6 ICMP and UDP statisticsfor the specified tunnel ID. The tunnel ID value ranges between 0 and 128.
- `<interface-type>` - Displays the IPv6 ICMP and UDP statistics 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.

- **<if-num>** - Displays the IPv6 ICMP and UDP statistics for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan. For example: 0/1 represents that the slot number is 0 and port number is 1.
- **<IP-interface-type>** - Displays the IPv6 ICMP and UDP statistics for the specified L3 Psuedo wire interface in the system.
- **<IP-interface-number>** - Displays the IPv6 ICMP and UDP 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.

   The maximum number of PseudoWire interfaces supported in the system is 100.

- **hc** - Displays the High counters for the ping messages.

Mode Privileged EXEC Model

Example

```
Your Product# show ipv6 traffic vrf default
     VRF   Name:          default
     ----------------

IPv6 Statistics
***************
0    Rcvd          0   HdrErrors
0    AddrErrors    0   FwdDgrams     0   UnknownProtos
0    Discards      7   Delivers      11   OutRequests
0    OutDiscards   0   OutNoRoutes   0   ReasmReqds
```

```
0    ReasmOKs       0    ReasmFails
  Sent:  0    FragOKs     0    FragFails    0  FragCreates
0    RcvdMCastPkt  5    SentMcastPkts 0    TruncatedPkts
0    RcvdRedirects        0    SentRedirects


      0    InOctets  0    InNoRoutes     0  OutFwdDatgrms
      0    OutFrgRqds    0  OutTrnsmit     0    OutOctets
      0  InMcstOctets  0  OutMcastOctets  0  InBcstPkts
      0  OutBcstPkts  0  DiscntTime    1000  RefrshRate
    ICMP Statistics
    ***************
    Received :
0 ICMPPkts    0 ICMPErrPkt    0 DestUnreach   0 TimeExcds
0 ParmProbs   0 PktTooBigs 0 EchoReq   0 EchoReply
0 RouterSols 0 RouterAdv   0 NeighSols   0 NeighborAdv
0    NA_RFlagSet   0 NA_SFlagSet       0 NA_OFlagSet
0    Redirects     0 AdminProhib
     Sent
0 ICMPMsgs   0 ICMPErrMsgs   0 DstUnReach   0 TimeExcds
0 ParmProbs   0 PktTooBigs   0 EchoReq      0 EchoReply
0 RouterSols   0 RouterAdv   0 NeighSols   0 NeighborAdv
0    NA_RFlagSet   0 NA_SFlagSet       0 NA_OFlagSet
0    RedirectMsgs 0 AdminProhibMsgs    0 Rate-limited
    UDP statistics
    **************
    Received :
0 UDPDgrams     6 UDPNoPorts        0 UDPErrPkts
    Sent :
0 UDPDgrams
```

```
VRF   Name:          mgmt
----------------
    IPv6 Statistics
    ***************
2088    Rcvd          0   HdrErrors
0    AddrErrors    0   FwdDgrams     0   UnknownProtos
0    Discards      0   Delivers      11   OutRequests
0    OutDiscards   0   OutNoRoutes   0   ReasmReqds
0    ReasmOKs      0   ReasmFails
 Sent:  0  FragOKs     0  FragFails     0  FragCreates
 2088  RcvdMCastPkt  4  SentMcastPkts 0  TruncatedPkts
0    RcvdRedirects       0    SentRedirects
200370 InOctets     0 InNoRoutes     0 OutFwdDatgrms
  0   OutFrgRqds    4 OutTrnsmit    248 OutOctets
 200370 InMcstOctets  88 OutMcastOctets   0 InBcstPkts
    0 OutBcstPkts     0 DiscntTime   1000  RefrshRate
    ICMP Statistics
    ***************
    Received :
2085 ICMPPkts  0 ICMPErrPkt  0 DestUnreach  0 TimeExcds
0  ParmProbs  0 PktTooBigMsg  0 ICMPEchoReq  0 ICMPEchoReps
0 RouterSols   2085 RouterAdv    0 NeighSols    0 NeighAdv
0   NA_RFlagSet  0 NA_SFlagSet      0 NA_OFlagSet
0   Redirects    0 AdminProhib
  Sent
0 ICMPMsgs    0 ICMPErrMsgs     0 DstUnReach    0 TimeExcds
0 ParmProbs   0 PktTooBigs      0 EchoReq       0 EchoReply
1 RouterSols  0 RouterAdv      3 NeighSols    0 NeighborAdv
0   NA_RFlagSet  0 NA_SFlagSet      0 NA_OFlagSet
```

```
  0   RedirectMsgs 0 AdminProhibMsgs   0 Rate-limited
    UDP statistics
    **************
    Received :
156 UDPDgrams    3 UDPNoPorts       0 UDPErrPkts
    Sent :
0 UDPDgramst
```

Your Product(config)# show ipv6 traffic vrf default

```
      VRF   Name:          default
      ----------------
          IPv6 Statistics
          ***************
      7  Rcvd          0 HdrErrors
      0  AddrErrors    0  FwdDgrams     0  UnknownProtos
      0  Discards      7  Delivers      11 OutRequests
      0  OutDiscards   0  OutNoRoutes    0 ReasmReqds
      0    ReasmOKs      0   ReasmFails
       Sent: 0  FragOKs   0  FragFails   0  FragCreates
      0 RcvdMCastPkt  5 SentMcastPkts  0 TruncatedPkts
      0    RcvdRedirects       0    SentRedirects
        0 InOctets      0 InNoRoutes    0 OutFwdDatgrms
        0 OutFrgRqds   11 OutTrnsmit   1140 OutOctets
        0 InMcstOctets  128 OutMcastOctets  0 InBcstPkts
        0 OutBcstPkts   0 DiscntTime     1000 RefrshRate
          ICMP Statistics
          ***************
          Received :
      7 ICMPPkts 0 ICMPErrPkt  0 DestUnreach 0 TimeExcds
      0 ParmProbs 0 PktTooBigMsg 0 ICMPEchoReq 5 ICMPEchoReps
```

```
  0 RouterSols   0 RouterAdv   1 NeighSols     1 NeighAdv
0    NA_RFlagSet   1 NA_SFlagSet       1 NA_OFlagSet
0    Redirects     0 AdminProhib
     Sent
   5 ICMPMsgs   0 ICMPErrMsgs    0 DstUnReach    0 TimeExcds
   0 ParmProbs 0 PktTooBigs     5 EchoReq       0 EchoReply
   0 RouterSols 0 RouterAdv     5 NeighSols     1 NeighborAdv
    1    NA_RFlagSet   1 NA_SFlagSet       1 NA_OFlagSet
   0    RedirectMsgs 0 AdminProhibMsgs    0 Rate-limited
        UDP statistics
        **************
        Received :
   0 UDPDgrams     6 UDPNoPorts        0 UDPErrPkts
        Sent :
   0 UDPDgrams
```

Related Command(s)

- `clear ipv6 traffic` – Removes all the entries in the IPv6 traffic table.

33.31 ipv6 path mtu discover

Command Objective This command enables path mtu discovery for the node. Path MTU (Maximum Transmission Unit) discovery in IPv6 allows a host to dynamically discover and adjust to differences in the MTU size of every link along a given data path.

The no form of the command disables path mtu discovery.

Syntax

```
ipv6 [vrf <vrf-name>] path mtu discover

no ipv6 [vrf <vrf-name>] path mtu discover
```

Parameter Description

- `vrf <vrf-name>` - Configures the path mtu discovery on an interface for 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 enabled

- VRF instance should be created, before executing this command to configure the path mtu discovery on an interface in the context·
- VRF instance should be mapped to the IPV4 / IPV6 interface, before executing this command to configure the static routes for the context in the interface.

Example

```
Your Product(config)# ipv6 path mtu discover
```

Related Command(s)

- `ip vrf` –Creates VRF instance.
- `show ipv6 pmtu` –Displays the configured PMTU entries.
- `ip vrf forwarding` –Maps the IPV4 / IPV6 interface to the context.

33.32 ipv6 path mtu

Command Objective This command configures Maximum Transmission Unit (MTU) for usage in PMTU Discovery.

Every network link has a maximum packet size called the link's MTU (Maximum Transmission Unit). The full path from one system to another may travel across many links with different MTUs. The smallest MTU for all the links in a path is the path MTU.

The no form of the command removes MTU for usage in PMTU Discovery.

Syntax

```
ipv6 path mtu [vrf <vrf-name>] <prefix addr> <mtu>

ipv6 path mtu [vrf <vrf-name>] <prefix addr>
```

Parameter Description

- `vrf <vrf-name>` - Configures MTU for usage in PMTU discovery for specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
- `<prefix addr>` - Configures the destination IPv6 address.
- `<mtu>` - Configures the maximum transmission unit value. This value ranges between 1280 and 65535.

Mode Global Configuration Mode

Default mtu – 1500

☞

- VRF instance should be created, before executing this command to configure MTU for usage in PMTU discovery in the context.
- VRF instance should be mapped to the IPV4 / IPV6 interface, before executing this command to configure the static routes for the context in the interface.

Example

```
Your Product(config)# ipv6 path mtu 11::22 3200
```

Related Command(s)

- `ip vrf` – Creates VRF instance.
- `show ipv6 pmtu` – Displays the configured PMTU entries.
- `show ipv6 interface` – Displays the IPv6 interfaces.
- `ip vrf forwarding` – Maps the IPV4 / IPV6 interface to the context.

33.33 show ipv6 pmtu

Command Objective This command displays the configured PMTU entries

Syntax `show ipv6 pmtu [vrf <vrf-name>]`

Parameter Description

- `vrf <vrf-name>` - Displays the configured PMTU Entries on an interface for 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

- VRF instance should be created, before executing this command to display configured PMTU entries in the context.
- VRF instance should be mapped to the IPV4 / IPV6 interface, before executing this command to configure the static routes for the context in the interface.

Example

```
Your Product# show ipv6 pmtu
    PMTU discovery is enabled in default
    PMTU discovery is enabled in mgmt
        Ipv6 Path MTU Table
        -------------------
    Vrf Name    Destination      PMTU
    --------    -----------      ----
    default         11::22                          3200
```

Related Command(s)

- `ip vrf` – Creates VRF instance.
- `ipv6 path mtu` – Configures Maximum Transmission Unit for usage in PMTU Discovery.
- `ipv6 path mtu discover` – Enables path mtu discovery for the node.
- `ip vrf forwarding` – Maps the IPV4 / IPV6 interface to the context

33.34 ipv6 interface-identifier

Command Objective This command configures 64 bit IPv6 identifier on the interface. The Interface Identifier is combined with an address prefix to form an interface address. The prefix value ranges between 0 and 64 bits.

The no form of the command deletes IPv6 interface identifier.

Syntax

```
ipv6 interface-identifier <prefix>

no ipv6 interface-identifier <prefix>
```

Mode Interface configuration Mode (Vlan/ Router)

Default IPv6 interface identifier is configured

Example

```
Your Product(config)# ipv6 interface-identifier ::3311
```

Related Command(s)

- `show ipv6 interface` – Displays the IPv6 interfaces.

33.35 ipv6 icmp error-interval

Command Objective This command configures ICMPv6 (Internet Control Message Protocol) error rate limit for limiting the rate at which IPv6 ICMP error messages are sent out on the network. The maximum number of tokens allowed in the bucket can be specified, and for every error message to be sent, one token is removed from the bucket. If a series of error messages is generated, error messages can be sent until the bucket is empty. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket.

The no form of the command removes ICMPv6 error rate limit.

Syntax

```
ipv6 icmp error-interval <milliseconds(1-65535)>
[<bucketsize(1-200)>]

no ipv6 icmp error-interval
```

Parameter Description

- `<milliseconds(1-65535)>` - Configures the time interval between tokens being placed in the bucket. This value ranges between 1 and 65535.
- `<bucketsize(1-200)>` - Configures the maximum number of tokens stored in the ICMPv6 bucket. This value ranges between 1 and 200.

Mode Interface configuration Mode (Vlan/ Router)

Default

- ICMPv6 error rate limiting is enabled.
- milliseconds - 100
- bucketsize - 10

Example

```
Your Product(config)# ipv6 icmp error-interval 65534 178
```

Related Command(s)

- `show ipv6 interface` – Displays the IPv6 interfaces.

33.36 ipv6 icmp dest-unreachable

Command Objective This command enables or disables ICMPv6 destination unreachable messages on the interface that has been configured.

When a ping ECHO request is sent, and if the destination is not reachable, then the reply is sent with destination unreachable flag enabled. Thereby this error messages can be sent or dropped using this command.

The ICMP Unreachable Destination Counters feature enables to clear and display packets that have been discarded because of an unreachable destination, and to configure a threshold interval for triggering error messages.

Syntax `ipv6 icmp dest-unreachable { enable | disable }`

Parameter Description

- `enable` - Enables ICMPv6 destination unreachable messages on the interface.
- `disable` - Disables ICMPv6 destination unreachable messages on the interface.

Mode Interface configuration Mode (Vlan/ Router)

Default ICMPv6 destination unreachable error messages are enabled

---

Example

```
Your Product(config-if)# ipv6 icmp dest-unreachable enable
```

Related Command(s)

- `show ipv6 interface` – Displays the IPv6 interfaces.

33.37 ipv6 policy-prefix

Command Objective This command configures IPv6 prefix in the policy table. This table is used for default address selection in IPv6 and to configure the precedence and label associated with a source or destination address.

The no form of the command deletes the Ipv6 prefix from the policy table.

Syntax

```
ipv6 policy-prefix <prefix> <prefix Len> precedence
<integer> label <integer>

no ipv6 policy-prefix <prefix> <prefix Len> precedence
<integer> label <integer>
```

Parameter Description

- `<prefix>` - Configures the IPv6 Address for which the policy needs to be configured.
- `<prefix Len>` - Configures the number of high-order bits in the IPv6 address. These bits are common among all hosts within a network. This value ranges between 0 and 128.
- `precedence <integer>` - Configures the precedence value associated with the address in the policy table which is the prefix for sorting destination addresses. The precedence is higher for higher value. This value ranges between 1 and 128.
- `label <integer>` - Configures label value of the prefix associated with the address in the policy table. This value ranges between 0 and 255.

Mode Interface configuration Mode (Vlan/ Router)

Default

- precedence - 30
- label – 2

- If the prefix length is ‘n’, then for the first ‘n’ number of bits, prefix should be greater than 0.

Example

```
Your Product(config-if)# ipv6 policy-prefix  22::44 53
precedence 2 label 3
```

Related Command(s)

- `show ipv6 addr-sel-policy-table` – Displays the address selection policy table

33.38 ipv6 compatible rfc5095

Command Objective This command configures IPv6 compatibility with RFC5095 which is used for the deprecation of routing headers of type 0.

The no form of the command disables IPv6 compatibility with RFC5095

Syntax

```
ipv6 compatible rfc5095 [vrf <vrf-name>]

no ipv6 compatible rfc5095 [vrf <vrf-name>]
```

Parameter Description

- `vrf <vrf-name>` - Configures the IPv6 compatibility with RFC5095 for 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 IPv6 compatibility with RFC5095 is enabled

- VRF instance should be created, before executing this command to configure IPv6 compatibility with RFC5095 in the context.
- VRF instance should be mapped to the IPV4 / IPV6 interface, before executing this command to configure the static routes for the context in the interface.

Example

```
Your Product(config)# ipv6 compatible rfc5095 vrf default
```

Related Command(s)

- `ip vrf` –Creates VRF instance.
- `vrf forwarding` – Maps the IPV4 / IPV6 interface to the context.

33.39 ipv6 unicast-routing – interface configuration

Command Objective This command enables unicast routing which is used for one to one communication across the ipv6 internet. An IPv6 unicast address is an identifier for a single interface, on a single node. A packet that is sent to a unicast address is delivered to the interface identified by that address.

The no form of the command disables unicast routing.

Syntax

```
ipv6 unicast-routing

no ipv6 unicast-routing
```

Mode Interface configuration Mode (Vlan/ Router)

Default Unicast routing is enabled

☞ The physical interface should be configured as router port, before executing this command for the physical interface.

Example

```
Your Product(config-if)# ipv6 unicast-routing
```

Related Command(s)

- `no switchport` – Configures the port as router port.
- `ipv6 hop-limit` – Configures the maximum hoplimit for all IPv6 packets originating from the interface.

33.40 ipv6 default scope-zone

Command Objective This command configures a default scope-zone for a particular scope.

Syntax

```
ipv6 default scope-zone {interfacelocal | linklocal |
subnetlocal | adminlocal | sitelocal | scope6 | scope7 |
orglocal | scope9 | scopeA | scopeB | scopeC | scopeD }
<zone-index>
```

Parameter Description

- `interfacelocal` - Configures zone for interface local scope on the interface. This scope spans only a single interface on a node and is useful only for loopback transmission of multicast.
- `linklocal` - Configures zone for link local scope on the interface.This scope is applicable for unicast/anycast addresses.
- `subnetlocal` - Configures zone for subnet local scope on the interface.
- `adminlocal` - Configures zone for admin local scope on the interface. This is the smallest scope that must be not automatically derived from physical connectivity or other non-multicast-related configuration.
- `sitelocal` - Configures zone for site local scope which is intended to span a single site on the interface.
- `scope6` - Configures default scope-zone for scope 6 on the interface.
- `scope7` - Configures default scope-zone for scope 7 on the interface.
- `orglocal` - Configures zone for organisation local which is intended to span multiple sites belonging to a single organization on the interface.
- `scope9` - Configures default scope-zone for scope 9 on the interface.
- `scopeA` - Configures default scope-zone for scope A on the interface.
- `scopeB` - Configures default scope-zone for scope B on the interface.
- `scopeC` - Configures default scope-zone for scope C on the interface.
- `scopeD` - Configures default scope-zone for scope D on the interface.
- `<zone-index>` - Configures zone index. This value ranges between 1 and 65535. This is the instance of a specific scope uniquely within the system. The zone index is used to associate unambiguously an IPv6 address to a specific zone.

Mode Global Configuration Mode

☞ This command executes only if the scope zones is created on the interface.

Example

```
Your Product(config)# ipv6 scope-zone sitelocal 1
```

```
Your Product# ipv6 default scope-zone sitelocal 1
```

Related Command(s)

- `ipv6 scope-zone` –Creates IPv6 scope zone on an interface.
- `show ipv6 default scope-zone` –Displays the default scope-zone for a particular scope

---

33.41 ipv6 scope-zone

Command Objective This command creates IPv6 scope zone on an interface.

Scope is a 4-bit value that describes the scope of an IPV6 address. A unicast address can possibly have 2 scopes (Linklocal and Global) only and a multicast address can have a maximum of 11 scopes.

The no form of the command removes IPv6 scope zone on the interface

---

Syntax

```
ipv6 scope-zone {interfacelocal | linklocal | subnetlocal
| adminlocal | sitelocal | scope6 | scope7 | orglocal |
scope9 | scopeA | scopeB | scopeC | scopeD | global}
<zone-index>
```

```
no ipv6 scope-zone {interfacelocal | linklocal |
subnetlocal | adminlocal | sitelocal | scope6 | scope7 |
orglocal | scope9 | scopeA | scopeB | scopeC | scopeD |
global } <zone-index>
```

Parameter Description

- `interfacelocal` - Configures zone for interface local scope on the interface. This scope spans only a single interface on a node and is useful only for loopback transmission of multicast. interface. This scope spans only a single interface on a node and is useful only for loopback transmission of multicast.
- `linklocal` - Configures zone for link local scope on the interface. This scope is applicable for unicast/anycast addresses.
- `subnetlocal` - Configures zone for subnet local scope on the interface.
- `adminlocal` - Configures zone for admin local scope on the interface. This is the smallest scope that must be not automatically derived from physical connectivity or other non-multicast-related configuration.
- `sitelocal` - Configures zone for site local scope which is intended to span a single site on the interface.
- `scope6` - Configures zone for scope 6 on the interface.
- `scope7` - Configures zone for scope 7 on the interface.
- `orglocal` - Configures zone for organisation local which is intended to span multiple sites belonging to a single organization on the interface.
- `scope9` - Configures zone for scope 9 on the interface.
- `scopeA` - Configures zone for scope A on the interface.
- `scopeB` - Configures zone for scope B on the interface.
- `scopeC` - Configures zone for scope C on the interface.
- `scopeD` - Configures zone for scope D on the interface.

- **global** - Configures zone for global scope on the interface which is used for uniquely identifying interfaces anywhere in the Internet. This scope is applicable for unicast/ anycast addresses.
- **<zone-index>** - Configures zone index. This is the instance of a specific scope uniquely within the system. The zone index is used to associate unambiguously an IPv6 address to a specific zone. This value ranges between 1 and 65535.

Mode Interface configuration Mode (Vlan/ Router)lobal

Default

- scope-zone –linklocal and interfacelocal
- zone-index – 1

☞ On any interface, ipv6 scope-zone can be configured only after enabling ipv6 on it.

Example

```
Your Product(config)# interface vlan 3
Your Product(config-if)# ipv6 enable
Your Product(config-if)# ipv6 scope-zone sitelocal 1
Your Product(config)# interface vlan 2
Your Product(config-if)# ipv6 enable
Your Product(config-if)# ipv6 scope-zone scopeC 1
```

Related Command(s)

- **ipv6 enable** –Enables IPv6 processing on an interface.
- **ip pim component** –Configures the PIM component in the router.
- **show ipv6 zone** –Displays the interface associated with a scope-zone.

33.42 show ipv6 addr-sel-policy-table

Command Objective This command displays the address selection policy table which is used for default address selection.

Syntax `show ipv6 addr-sel-policy-table`

Mode Privileged EXEC Mode

Example

```
Your Product# show ipv6 addr-sel-policy-table
     IP6 PREFIX PREFIXLEN PRECEDENCE LABEL  ADDRTYPE
     ::              0       40      1        unicast
     ::              96      20      3        unicast
     ::1             128     50      0        unicast
     ::ffff:0:0      96      10      4        unicast
     2002::          16      30      2        unicast
```

Related Command(s)

- `ipv6 policy-prefix` –Configures IPv6 prefix in the policy table.

33.43 show ipv6 scope-zone interface

Command Objective This command displays the scope-zone configured on an interface.

Syntax

```
show ipv6 scope-zone [vrf <vrf-name>] [interface { vlan <vlan-id/vfi-id> [switch <switch-name>] | tunnel <tunnel-id> | <interface-type> <if-num> | <IP-interface-type> <IP-interface-number>} ]
```

Parameter Description

- `vrf <vrf-name>` - Displays the scope-zone configured on an interface for 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 scope-zone configured on an interface for the specified VLAN / VFI ID. This value ranges between 1 and 65535.
  - `<vlan –id>` - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094.
  - `<vfi-id>` - VFI ID is a VLAN created in the system which contains Pseudo wires and Attachment Circuits as member ports. This creates a logical LAN for the VPLS service. This value ranges between 4096 and 65535.

    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

    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 scope-zone configured on an interface for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature
- `tunnel <id>` - Displays the scope-zone configured on the specified tunnel interface. This value ranges between 0 and 128.
- `<interface-type>` - Displays the scope-zone 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.

- **<if-num>** - Displays the scope-zone 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.
- **<IP-interface-type>** - Displays the scope-zone in the specified L3 Psuedo wire interface in the system.
- **<IP-interface-number>** - Displays the scope-zone 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

- VRF instance should be created, before executing this command to display the scope-zone configured on an interface in the context.
- VRF instance should be created, before executing this command to display the scope-zone configured on an interface in the context.

Example

```
Your Product# show ipv6 scope-zone interface vlan 1

        Scope-Zones Interface Map Table

        VRF Id   : 0

        VRF Name: default

        Interface              Scope-Zones

       vlan1            interfacelocal1  linklocal1
```

Related Command(s)

- **ipv6 enable** –Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
- **ip vrf** –Creates VRF instance.
- **ipv6 scope-zone** –Creates IPv6 scope zone on an interface.

- `ip vrf forwarding` –Maps the IPV4 / IPV6 interface to the context.

33.44 show ipv6 zone - if-list

Command Objective This command displays the interface associated with a scope-zone.

Syntax `show ipv6 zone <Zone-Name> if-list [vrf <vrf-name>]`

Parameter Description

- `<Zone-Name>` - Displays the scope-zone name for which the interface list needs to be displayed.
- `vrf <vrf-name>` - Displays the interface associated with a scope-zone for 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

- VRF instance should be created, before executing this command to display interface associated with a scope-zone in the context.
- VRF instance should be mapped to the IPV4 / IPV6 interface, before executing this command to configure the static routes for the context in the interface.

Example

```
Your Product# show ipv6 zone interfacelocal1 if-list

                Scope-Zones          Interface

                interfacelocal1   vlan1
```

Related Command(s)

- `ip vrf` –Creates VRF instance.
- `ipv6 scope-zone` –Creates IPv6 scope zone on an interface.
- `ip vrf forwarding` –Maps the IPV4 / IPV6 interface to the context.

33.45 show ipv6 default scope-zone

Command Objective This command displays the default scope-zone for a particular scope.

Syntax `show ipv6 default scope-zone [vrf <vrf-name>]`

Parameter Description

- `vrf <vrf-name>` - Displays the scope-zone configured on an interface for 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

- VRF instance should be created, before executing this command to display the scope-zone configured on an interface in the context.
- VRF instance should be mapped to the IPV4 / IPV6 interface, before executing this command to configure the static routes for the context in the interface.

Example

```
Your Product# show ipv6 default scope-zone
```

Related Command(s)

- `ip vrf` –Creates VRF instance.
- `ipv6 scope-zone` –Creates IPv6 scope zone on an interface.
- `ipv6 default scope-zone` –Configures a default scope-zone for a particular scope.
- `ip vrf forwarding` –Maps the IPV4 / IPV6 interface to the context.

34 OSPFv3

Open Shortest Path First (OSPF) is a link-state, hierarchical Interior

Gateway Protocol (IGP) routing algorithm.

OSPFv3 is the modified form of OSPF to support version 6 of the Internet Protocol. The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, etc.) remain unchanged. However, some changes have been necessary, either due to changes in protocol semantics between IPv4 and IPv6, or simply to handle the increased address size of IPv6.

The list of CLI commands for the configuration of OSPFv3 is as follows:

- ipv6 router ospf
- router-id
- area - stub/nssa
- area - stability-interval
- area - translation-role
- timers spf
- abr-type
- area - default-metric value
- area - default-metric type
- area - virtual-link
- ASBR Router
- area - range
- area – summary-prefix
- redistribute
- distribute-list route-map in
- passive-interface
- route-calculation staggering
- route-calculation staggering-interval
- distance
- host - metric/area-id
- no area
- nssaAsbrDfRtTrans
- redist-config
- as-external lsdb-limit
- exit-overflow-interval
- demand-extensions

- reference-bandwidth
- nsf ietf restart-interval
- nsf ietf helper disable
- nsf ietf helper gracetimelimit
- nsf ietf helper strict-lsa-checking
- nsf ietf grace lsa ack required
- nsf ietf grace lsa retransmit-count
- nsf ietf restart-reason
- ipv6 ospf area
- ipv6 ospf demand-circuit
- ipv6 ospf retransmit-interval
- ipv6 ospf transmit-delay
- ipv6 ospf priority
- ipv6 ospf hello-interval
- ipv6 ospf dead-interval
- ipv6 ospf poll-interval
- ipv6 ospf metric
- ipv6 ospf network
- ipv6 ospf neighbor
- ipv6 ospf passive-interface
- • ipv6 ospf neighbor probing
- ipv6 ospf neighbor-probe retransmit-limit
- ipv6 ospf neighbor-probe interval
- • debug ipv6 ospf - pkt
- show ipv6 ospf - interface
- show ipv6 ospf - neighbor
- show ipv6 ospf virtual-links
- show ipv6 ospf - request/retrans-list
- show ipv6 ospf border-routers
- show ipv6 ospf - area-range / summary-prefix
- show ipv6 ospf - General Information
- show ipv6 ospf - LSA Database
- show ipv6 ospf - route
- show ipv6 ospf - areas
- show ipv6 ospf - host

- show ipv6 ospf - redist-config
- show ipv6 ospf redundancy
- ipv6 ospf linkLSASuppress

34.1 ipv6 router ospf

Command Objective This command enables the OSPFv3 routing protocol, if the VRF instance name is not specified. This command creates the OSPF instance, if the VRF instance name is specified.

The no form of the command disables the OSPFv3 routing protocol, if the VRF instance name is not specified. The no form of the command deletes the OSPF instance, if the VRF instance name is specified.

Syntax

```
ipv6 unicast-routing [vrf <vrf-name>]
no ipv6 unicast-routing [vrf <vrf-name>]
```

Parameter Description

- `vrf<vrf-name>` - Configures ipv6 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

- Enabled

- VRF instance should be created, before executing this command to configure the unicast routing in the context.

Example

```
Your Product(config)# ipv6 unicast-routing
```

Related Command(s)

- `iv6 router rip / ipv6 router rip` – name - Enables RIP6 and enters into the router configuration Mode
- `ip vrf` - Creates VRF instance
- `redistribute` - Configures the protocol from which the routes have to be redistributed into OSPFv3
- `distribute-list route-map in` - Enables inbound filtering for routes
- `route-calculation staggering` - Enables OSPFv3 route calculation staggering
- `route-calculation staggering-interval` - Configures the OSPFv3 route calculation staggering interval

- **distance** - Enables the administrative distance of the routing protocol and sets the administrative distance value
- **nsf ietf restart-interval** - Enables the graceful restart support and configures grace interval
- **nsf ietf helper disable** - Disables the helper support
- **nsf ietf helper gracetimelimit** - Configures the helper grace time limit
- **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 grace lsa retransmit-count** - Configures the maximum number of retransmissions for unacknowledged GraceLSA
- **nsf ietf restart-reason** - Configures the reason for restart
- **ipv6 ospf area** – Enables OSPFv3 for IPv6 on an interface
- **debug ipv6 ospf** - pkt – Sets the trace levels
- **show ipv6 ospf - request/retrans-list** - Displays the list of all link state advertisements (LSAs) in request-list or in retransmission-list
- **ipv6 ospf linkLSASuppress** – Configures the interface to suppress Link LSA origination

---

34.2 router-id

Command Objective This command configures router ID which is a unique 32-bit number of the router in the AS. If a router OSPF Router ID is changed, it results in disabling the OSPFv3 protocol, updating the Router ID and then enabling the OSPFv3 protocol.

Syntax `router-id <IPv4-Address>`

Mode Router Configuration Mode

Example

```
Your Product(config-router)# router-id 11.0.0.1
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `ipv6 ospf area` – Enables OSPFv3 for IPv6 on an interface.
- `export ospf` – Enables redistribution of Ospf area/External routes to protocol.
- `show ipv6 ospf - General Information` – Displays general information about the OSPFv3 routing process

---

34.3 area - stub/nssa

Command Objective This command defines an area as a stub area or an NSSA (Not So Stubby Area)

Syntax `area <area-id> {{ stub | nssa } [no-summary]}`

Parameter Description

- `<area-id>` - Configures a 32-bit integer area id where the host belongs. If the area Id is not configured, the host is associated to the backbone area
- `stub` - Configures a Stub area which stores the router LSA, Network LSA, Inter Area Prefix LSA, Intra Area Prefix LSA and the Link LSA in the database.
- `nssa` - Configures Not So Stubby Area which is a proprietary extension of the existing stub area feature that allows the injection of external routes in a limited fashion into the stub area.
- `no-summary` - Allows an area to be a stubby/not-so-stubby but does not allow it to have summary routes injected into it

Mode Router Configuration Mode

Example

```
Your Product(config-router)# area 1.1.1.1 stub no-summary
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `area` - translation-role - Configures the translation role for NSSA.
- `area - default-metric` - Sets the default metric value for an area of type NSS.
- `area - default-metric type` - Sets the default metric-type for an area type of NSS.
- `area – range` - Creates the Internal Aggregation Address Range.
- `area - summary-prefix` - Enables route aggregation/filtering while importing routes in the OSPFv3 domain.
- `host – metric/area-id` - Configures a host entry area-id.
- `show ipv6 ospf areas` – Displays the Area Table.

34.4 area - stability-interval

Command Objective

This command configures the stability interval (in seconds) for the NSSA.

The no form of the command sets the default value of the stability interval for the NSSA.

Syntax

```
area <area-id> stability-interval <interval-value (1-65535)>

no area <area-id> stability-interval
```

Parameter Description

- `<area-id>` - Configures a 32-bit integer area id where the host belongs. If the area Id is not configured, the host is associated to the backbone area
- `stability-interval<interval-value>` - Configures the number of seconds after which an elected translator determines that its services are no longer required, and that it must continue to perform its translation duties. This value ranges between 1 and 65535.

Mode

Router Configuration Mode

Example

```
Your Product(config-router)# area 0.0.0.1 stability-interval 50
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf areas` – Displays the Area Table.

34.5 area - translation-role

Command Objective

This command configures the translation role for NSSA.

The no form of the command configures the default translation role for the NSSA.

Syntax

```
area <area-id> translation-role { always | candidate }

no area <area-id> translation-role
```

Parameter Description

- `<area-id>` - Configures a 32-bit integer area id where the host belongs. If the area Id is not configured, the host is associated to the backbone area
- `translation-role` - Configures an NSSA Border router's ability to perform NSSA Translation of Type-7 LSAs to Type-5 LSAs. The options are:
- `always` – When the translator role is set to always, the Type-7 LSAs are always translated into Type-5 LSAs.
- `candidate` - When translator role is set to candidate, an NSSA border
- router participates in the translator election process.

Mode

Router Configuration Mode

Default

translation-role - candidate

This command executes only if the area is set as NSSA.

Example

```
Your Product(config-router)# area 1.1.1.1 translation-role
always
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `area – stub/nssa` - Defines an area as NSSA.
- `show ipv6 ospf areas` – Displays the Area Table.

34.6 timers spf

Command Objective

This command configures the delay time and the hold time between two consecutive SPF calculations. Delay time is the time interval when OSPFv3 receives a topology change and when it starts a Shortest Path First (SPF) calculation.

The no form of the command sets the default values for spf-delay and spf-holdtime.

Syntax

```
timers spf <spf-delay> <spf-holdtime>

no timers spf
```

Parameter Description

- `<spf-delay>` - Configures the interval by which SPF calculation is delayed after a topology change reception. This value ranges between 0 and 65535.
- `<spf-holdtime>` - Configures the delay between two consecutive SPF calculations. This value ranges between 0 and 65535.

Mode

Router Configuration Mode

Default

- spf-delay - 5 seconds
- spf-holdtime - 10 seconds

Example

```
Your Product(config-router)# timers spf 10 20
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf - General Information` – Displays general information about the OSPFv3 routing process.

34.7 abr-type

Command Objective This command sets the ABR (Area Border Router) type.

The no form of the command sets the default ABR type.

Syntax

```
abr-type { standard | cisco | ibm }
no abr-type
```

Parameter Description

- `standard` - Sets the ABR (Area Border Router) type as Standard ABR type.
- `cisco` - Sets the ABR (Area Border Router) type as CISCO ABR type.
- `ibm` - Sets the ABR (Area Border Router) type as IBM ABR type.

Mode Router Configuration Mode

Default standard

Example

```
Your Product(config-router)# abr-type cisco
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf - General Information` – Displays general information about the OSPFv3 routing process.

34.8 area - default-metric value

Command Objective This command sets the default metric value for an area of type NSS/stub only.

Syntax `area <area-id> default-metric <metric>`

Parameter Description

- `<area-id>` - Configures a 32-bit integer area id where the host belongs. If the area Id is not configured, the host is associated to the backbone area.
- `default-metric <metric>` - Configures the cost metric for the redistributed routes. This value ranges between 1 and 16777214. This command does not apply to directly connected routes. Use a route map to set the default metric for directly connected routes.

Mode Router Configuration Mode

Default metric - 1

☞ Default metric can be defined only for a valid area. This command executes only if the area is set as NSSA.

Example

```
Your Product(config-router)# area 1.1.1.1 default-metric
20
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `area – stub/nssa` - Defines an area as NSSA.

34.9 area - default-metric type

Command Objective This command sets the default metric-type for an area type of NSS/stub only.

Syntax `area <area-id> default-metric type <metricType>`

Parameter Description

- `<area-id>` - Configures a 32-bit integer area id where the host belongs. If the area Id is not configured, the host is associated to the backbone area.
- `default-metric type<metricType>` - Configures the type of metric.

Mode Router Configuration Mode

Default metricType - 1

☞ Default metric can be defined only for a valid area. This command executes only if the area is set as NSSA.

Example

```
Your Product(config-router)# area 1.1.1.1 default-metric
type 2
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `area – stub/nssa` - Defines an area as NSSA.
- `area - stub/nssa` – Defines an area as a stub area or an NSSA (Not So Stubby Area)

34.10 area - virtual-link

Command Objective

This command sets the Virtual Link between areas.

In OSPFv3, all areas must be connected to a backbone area. If there is a break in backbone continuity, or the backbone is purposefully partitioned, a virtual link can be established. The two endpoints of a virtual link are ABRs. The virtual link must be configured in both routers. The configuration information in each router consists of the other virtual endpoint (the other ABR) and the non-backbone area that the two routers have in common (called the transit area).

If 20.0.0.3 is the Router ID of the Neighbor and 100 is the Interface Index assigned to the OSPFv3 virtual interface, then this interface index is advertised in Hello packet sent over the virtual link and in the router's router-LSAs.

Syntax

```
area <area-id> virtual-link <router-id> <if-index> [hello-interval <seconds>] [retransmit-interval <seconds>] [transmit-delay <seconds>] [dead-interval <seconds>]
```

Parameter Description

- `<area-id>` - Configures a 32-bit integer area id where the host belongs. If the area Id is not configured, the host is associated to the backbone area.
- `<router-id>` - Configures the Router ID of the Virtual Neighbor.
- `<if-index>` - Configures the interface Index assigned to the OSPFv3 virtual interface. This value ranges between 1 and 214783647.
- `hello-interval<seconds>` - Configures the interval between hello packets on the OSPFv3 virtual link interface. This value ranges between 1 and
- 65535 seconds.
- `retransmit-interval<seconds>` - Configures the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPFv3 virtual link interface. This value ranges between 1 and 1800 seconds.
- `transmit-delay<seconds>` - Configures the estimated time it takes to transmit a link state update packet over this interface. This value ranges between 1 and 1800 seconds.
- `dead-interval<seconds>` - Configures the interval at which hello packets must not be seen before its neighbors declare the router down. This value ranges between 1 and 65535 seconds.

Mode

Router Configuration Mode

Default

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

☞ Virtual links cannot be configured through stub areas.

☞ Hello-interval and dead-interval values must be the same for all routers on a specific network.

Example

```
Your Product(config-router)# area 1.1.1.1 virtual-link
20.0.0.3 1 hello-interval 50 retransmit-interval 6
transmit-delay 6 dead-interval 100
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf interface` – Displays the OSPFv3-related interface information.
- `show ipv6 ospf virtual-links` – Displays the parameters and the current state of OSPFv3 virtual links.

34.11 ASBR Router

Command Objective This command configures the router as an ASBR.

The no form of the command disables the ASBR status of the router.

Syntax

```
ASBR Router
no ASBR Router
```

Mode Router Configuration Mode

☞ Only when ASBR (Autonomous System Border Router) status is configured to enable, routes from other protocols are redistributed into OSPFv3 domain.

Example

```
Your Product(config-router)# ASBR Router
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `redistribute` - Configures the protocol from which the routes have to be redistributed into OSPFv3.
- `redist-config` - Configures the information to be applied to routes learnt from RTM.
- `show ipv6 ospf - General Information` – Displays general information about the OSPFv3 routing process.

34.12 area - range

Command Objective This command creates the Internal Aggregation Address Range.

The Internal Address Range is of two types:

- Type-3 Aggregation
- Type 7 Translation Aggregation

Syntax

```
area <Area-ID> range <IPv6-Prefix> <Prefix-Length>
[{ advertise | not-advertise }] {summary | Type7} [tag
<tag-value>]
```

Parameter Description

- `<Area-ID>` - Configures a 32-bit integer area id where the host belongs. If the area Id is not configured, the host is associated to the backbone area.
- `<IPv6-Prefix>` - Configures the IPv6 address prefix of the range.
- `<Prefix-Length>` - Configures the prefix length of the address range. This value ranges between 0/7-128.
- `advertise` - Flushes out all the routes (LSAs) falling in the range and generates aggregated LSA for the range.
- `not-advertise` - Suppresses routes that match the prefix/prefix-length pair.
- `summary` - Sets the type as Summary LSA.
- `Type7` - Sets the type as Type-7 LSA.
- `tag<tag-value>` - Sets the tag value for the aggregated route.

Mode Router Configuration Mode

Default tag - 0

☞ This command executes only if the area is set as NSSA. When parameter summary is specified, the configured range is used for aggregating Type-3 LSA. When parameter Type7 is specified, the configured range is used for aggregating Type-7 LSAs. The optional parameter tag is used to set the tag value for the aggregated route. This is not used by the OSPFv3 protocol alone. It can be used to communicate information between AS boundary routers.

Example

```
Your Product(config-router)# area 0.0.0.0 range
3ffe:5000:481d::5 80 advertise Type7 tag 20
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.

- `area – stub/nssa` - Defines an area as NSSA.
- `show ipv6 ospf - area-range / summary-prefix` – Displays either the list of all area address ranges information or all external summary address configuration information.

34.13 area – summary-prefix

Command Objective This command enables route aggregation/filtering while importing routes in the SPFv3 domain. The command configures Type-5 and Type-7 Address Range specifying whether Type-5/Type-7 LSAs are generated or not for the configured range for the particular area.

Syntax

```
area <AreaID> summary-prefix <IPv6-Prefix> <Prefix-Length>
[{ allowAll | denyAll | advertise | not-advertise}]
[Translation { enabled | disabled }]
```

Parameter Description

- `<Area-ID>` - Configures a 32-bit integer area id where the host belongs. If the area Id is not configured, the host is associated to the backbone area.
- `<IPv6-Prefix>` - Configures the IPv6 address prefix of the range.
- `<Prefix-Length>` - Configures the prefix length of the address range. This value ranges between 0/7-128.
- `allowAll` - Generates aggregated Type-5 LSAs for the specified range when set to allow All and the associated areaId is 0.0.0.0. In addition, aggregated Type-7 LSAs are generated in all the attached NSSAs for the specified range.
- `denyAll` - Generates neither Type-5 LSA nor Type-7 LSAs for the specified range.
- `advertise` - Generates Aggregated Type-5 LSAs when the associated areaId is 0.0.0.0. Otherwise, if the associated areaId is x.x.x.x (other than 0.0.0.0), aggregated Type-7 LSA is generated in NSSA area x.x.x.x.
- `not-advertise` - Does not generate Type-5 LSA for the specified range when the associated areaId is 0.0.0.0, while all the NSSA LSAs within this range are flushed out and aggregated Type-7 LSA is generated in all attached NSSAs. If associated areaId is x.x.x.x (other than 0.0.0.0), Type-7 LSA is not generated in NSSA x.x.x.x for the specified range.
- `Translation` - Sets translation of Type5 or Type 7 messages in the specified range The options are.
- `enabled` - Sets the P-Bit in the generated Type-7 LSA.
- `disabled` – Clears the P-Bit in the generated Type-7 LSA for the range.

Mode Router Configuration Mode

Default

- Translation-enabled
- advertise

☞ This command executes only if the area is set as NSSA. The Value allowAll/denyall is not valid for areaId other than 0.0.0.0.

Example

```
Your Product(config-router)# area 0.0.0.0 summary-prefix 1111::2222 advertise Translation enabled
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `area – stub/nssa` - Defines an area as NSSA.
- `show ipv6 ospf - area-range / summary-prefix` – Displays either the list of all area address ranges information or all external summary address configuration information.

34.14 redistribute

Command Objective

This command configures the protocol from which the routes have to be redistributed into OSPFv3.

The no form of the command disables the redistribution of routes from the given protocol into OSPFv3.

Syntax

```
redistribute {static | connected | ripng | bgp} [route-map <string(20)>]

no redistribute {static | connected | ripng | bgp } [route-map <string(20)>]
```

Parameter Description

- `static` - Advertises routes, configured statically in the OSPFv3 routing process.
- `connected` - Advertises directly connected networks routes in the OSPFv3 routing process.
- `ripng` - Advertises routes that are learnt by the RIP process in the OSPFv3 routing process.
- `bgp` - Advertises routes that are learnt by the BGP process in the OSPFv3 routing process.
- `route-map<string(20)>` - Identifies the specified route-map in the list of route-redistribution of routes to OSPFv3. This value is a string of size 20.

Mode

Router Configuration Mode

☞ This command executes only if the router is configured as ASBR. OSPFv3 routing protocol should be enabled, before executing this command.

To configure Redistribution of routes from other protocols, the following steps must be performed.

- Configure the router as ASBR.
- Configure redistribution of routes from particular protocol.

The above order must be maintained and ASBR setting must be done before enabling redistribution.

Example

```
Your Product(config-router)# redistribute static
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `ASBR Router` – Configures the router as an ASBR.
- `show ipv6 ospf - General Information` – Displays general information about the OSPFv3 routing process.

34.15 distribute-list route-map in

Command Objective

This command enables inbound filtering for routes specified by the route map name. This value is a string whose maximum size is 20.

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
```

Mode

Router Configuration Mode

☞ OSPFv3 routing protocol should be enabled, before executing this command.

Only one route map can be set for inbound routes. Another route map can be assigned, only if the already assigned route map is disabled.

Example

```
Your Product(config-router)# distribute-list route-map
rmap-test in
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show running-config ospf3` - Displays the current operating configuration in the system.

34.16 passive-interface

Command Objective

This command sets the global default passive interface status. All the interfaces created only after executing this command become passive interfaces.

The no form of the command resets the global default passive interface status. All the interfaces created only after executing this command become non-passive interfaces.

Syntax

```
passive-interface
no passive-interface
```

Mode

Router Configuration Mode

Default

Disabled

Example

```
Your Product(config-router)# passive-interface
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf - General Information` – Displays general information about the OSPFv3 routing process.

34.17 route-calculation staggering

Command Objective	This command enables OSPFv3 route calculation staggering and also sets the staggering interval to the last configured value. This feature staggers the OSPFV3 route calculation at regular intervals for processing neighbor keep alive and other OSPFV3 operations. The no form of the command disables OSPFv3 route calculation staggering and removes the staggering interval.

Syntax	`route-calculation staggering`
	
	`no route-calculation staggering`

Mode	Router Configuration Mode
Default	OSPFv3 route calculation staggering is enabled
Example	`Your Product(config-router)# route-calculation staggering`

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `route-calculation staggering-interval` – Configures the OSPFv3 route calculation staggering interval.
- `show ipv6 ospf - General Information` – Displays general information about the OSPFv3 routing process.

34.18 route-calculation staggering-interval

Command Objective This command configures the OSPFv3 route calculation staggering interval (in milliseconds). This value represents the time after which the route calculation is suspended for doing other OSPFv3 operations. This value ranges from 1000 to 214783647.

Syntax `route-calculation staggering-interval <milli-seconds (1000-2147483647)>`

Mode Router Configuration Mode

Default 10000 milliseconds (OSPF route calculation staggering interval is equal to Hello interval)

☞ This command executes only if OSPFv3 routing protocol and OSPv3 route calculation staggering are enabled

---

Example

```
Your Product(config-router)# route-calculation staggering-interval 2000
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `route-calculation staggering` - Enables OSPFv3 route calculation staggering.
- `show ipv6 ospf - General Information` – Displays general information about the OSPFv3 routing process.
- `show running-config ospf` - Displays the current operating configuration in the system.

34.19 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.

This distance value will not be used for distribute list. The administrative distance can be enabled for only one route map. The distance should be disabled for the already assigned route map, if distance needs to be enabled 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

- `name-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 of size 20.

Mode

Router Configuration Mode

Default

110 (Represents OSPF route)

☞ OSPFv3 routing protocol should be enabled, before executing this command

---

Example

```
Your Product(config-router)# distance 10 route-map rmap test
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show running-config ospf` - Displays the current operating configuration in the system.

34.20 host - metric/area-id

Command Objective This command configures a host entry with metric and/or area-id.

The no form of the command deletes a host entry.

Syntax

```
host <IPv6-Address> metric <cost> [area-id {<AreaID>}]
no host <IPv6-Address>
```

Parameter Description

- `<IPv6-Address>` - Configures the host entry with metric and/or area-id for the specified IPV6 address prefix.
- `metric <cost>` - Configures a metric value to be advertised.
- `area-id<AreaID>` - Configures a 32-bit integer area id where the host belongs. If the area Id is not configured, the host is associated to the backbone area.

Mode Router Configuration Mode

☞ To configure a host entry with area-id the area should be configured as NSSA in prior.

Example

```
Your Product(config-router)# host 3ffe:481d::5 metric 10
area-id 0.0.0.1
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `area – stub/nssa` - Defines an area as NSSA.
- `show ipv6 ospf host` – Displays the Host Table information.

34.21 no area

Command Objective This command deletes an area and does any one of the following based on the optional parameter.

- Coverts stub/nss area to normal area.
- Deletes virtual link.
- Deletes stub cost.
- Delete area-range or summary-prefix.

Syntax

```
no area <area-id> [ { stub | nssa | virtual-link
<router-id> | default-metric | {range {summary | Type7}
| summary-prefix} <IPv6-Prefix> <Prefix-Length>} ]
```

Parameter Description

- `<area-id>` - Configures a 32-bit integer area id where the host belongs. If the area Id is not configured, the host is associated to the backbone area.
- `stub` - Configures a Stub area which stores the router LSA, Network LSA, Inter Area Prefix LSA, Intra Area Prefix LSA and the Link LSA in the database.
- `nssa` - Configures Not So Stubby Area which is a proprietary extension of the existing stub area feature that allows the injection of external routes in a limited fashion into the stub area.
- `virtual-link <router-id>` - Configures the Router ID of the virtual neighbor.
- `Default-metric` - Sets the cost for the default summary route in a stub/NSS area.
- `range` - Sets the range. The options are:
  - Summary - Sets the range for summary.
  - Type7- Sets the range for Type7.
- `summary-prefix` - Configures the summary prefix.
- `<IPv6-Prefix>` - Configures the IPv6 address prefix of the range.
- `<Prefix-Length>` - Configures the prefix length of the address range.

Mode Router Configuration Mode

☞ Before deleting an area, it is necessary to delete all the interfaces attached to that area.

Example

```
Your Product(config-router)# no area 1.1.1.1

Your Product(config-router)# no area  1.1.1.1 stub

Your Product(config-router)# no area 1.1.1.1 default-
metric
```

```
Your Product(config-router)# no area 1.1.1.1 virtual-link
20.0.0.3

Your Product(config-router)# no area 1.1.1.1 range summary
3ffe:3010:481d::5  80
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf areas` – Displays the Area Table.
- `show ipv6 ospf - area-range / summary-prefix` – Displays either the list of all area address ranges information or all external summary address configuration information
- `no ipv6 ospf area` – Disables OSPFv3 routing protocol on the interface

34.22 nssaAsbrDfRtTrans

Command Objective

This command enables setting of P bit in the default Type-7 LSA generated by an NSSA internal ASBR.

The no form of the command disables setting of P bit in the default Type-7 LSA generated by an NSSA internal ASBR.

Syntax

```
nssaAsbrDfRtTrans
no nssaAsbrDfRtTrans
```

Mode

Router Configuration Mode

Default

Disabled

Example

```
Your Product(config-router)# nssaAsbrDfRtTrans
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf - General Information` – Displays general information about the OSPFv3 routing process.

34.23 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 <IPv6-Prefix> <Prefix-Length> [metric-value <metric>] [metric-type {asExttype1 | asExttype2}] [tag <tag-value>]

no redist-config <IPv6-Prefix> <Prefix-Length>
```

Parameter Description

- `<IPv6-Prefix>` - Sets the IPv6 address prefix.
- `<Prefix-Length>` - Sets the prefix length of the address.
- `metric-value <metric>` - Sets the metric value applied to the route before it is advertised into the OSPFv3 Domain.
- `metric-type` - Sets the metric Type applied to the route before it is advertised into the OSPFv3 Domain
- `asExttype1` - Denotes that the metric is advertised as AS-External type 1.
- `asExttype2` - Denotes that the metric is advertised as AS-External type 2.
- `tag <tag-value>` - Sets the tag type which describes whether Tags will be automatically generated or will be manually configured.

Mode

Router Configuration Mode

☞ This command executes only if Tag – ASBR Router is configured.

Example

```
Your Product(config-router)# redist-config 3ffe:5000:481d::5 80 metric-value 30 metric-type asExttype1 tag 12
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `ASBR Router` – Configures the router as an ASBR.
- `show ipv6 ospf redist-config` – Displays the configuration information to be applied to the routes learnt from the RTM.

34.24 as-external lsdb-limit

Command Objective This command sets the maximum number of non-Default AS-external-LSA entries that can be stored in the link-state database. This value ranges between -1 and 2147483647. If the value is -1, then there is no limit.

Syntax `as-external lsdb-limit <lsdb-limit (-1 - 2147483647)>`

Mode Router Configuration Mode

Default lsdb-limit - -1

When the number of non-Default AS-external-LSAs in a router's link-state database reaches the configured limit, the router enters Overflow- State. The router never holds more than the configured non-Default AS-external-LSAs in its database.

The LSDB limit MUST be set identically in all routers attached to the OSPFv3 backbone and/or any regular OSPFv3 area. (i.e. OSPFv3 stub areas and NSSAs are excluded).

Example

```
Your Product(config-router)# as-external lsdb-limit 10
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf - General Information` – Displays general information about the OSPFv3 routing process.
- `exit-overflow-interval` – Sets the number of seconds after which a router will attempt to leave the Overflow State.

34.25 exit-overflow-interval

Command Objective	This command sets the number of seconds after which a router will attempt to leave the Overflow State. This value ranges between 0 and 4199999999.
Syntax	`exit-overflow-interval <interval>`
Mode	Router Configuration Mode
Default	interval - 0
Example	`Your Product(config-router)# exit-overflow-interval 10`

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf - General Information` – Displays general information about the OSPFv3 routing process.

34.26 demand-extensions

Command Objective This command enables routing support for demand routing.

The no form of the command disables routing support for demand routing.

Syntax

```
demand-extensions
no demand-extensions
```

Mode Router Configuration Mode

Default Enabled

Example

```
Your Product(config-router)# demand-extensions
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf - General Information` – Displays general information about the OSPFv3 routing process.

34.27 reference-bandwidth

Command Objective This command sets the reference bandwidth in kilobits per second for calculating the default interface metrics. This value ranges between 0 and 4199999999.

Syntax `reference-bandwidth <ref-bw>`

Mode Router Configuration Mode

Default ref-bw - 100,000 KBPS

Example

```
Your Product(config-router)# reference-bandwidth 1000000
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf - General Information` – Displays general information about the OSPFv3 routing process.

34.28 nsf ietf restart-interval

Command Objective

This command enables the graceful restart support and configures the grace interval.

The no form of the command disables the graceful restart support and resets the grace interval to default value.

Syntax

```
nsf ietf [restart-interval <grace period (1-1800)>]
[plannedOnly]

no nsf ietf [restart-interval <integer (1-1800)>]
```

Parameter Description

- `restart-interval <grace period (1-1800)>` - Sets an interval during which the router can reacquire OSPFv3 neighbors that are fully operational prior to the restart. This value ranges between 1 and 1800 seconds. This interval 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.
- `plannedOnly` - Supports only the planned restarts (such as restarting a control plane after a planned downtime).

Mode

Router Configuration Mode

Default

- Graceful restart support is disabled.
- restart-interval - 120

☞ OSPFv3 routing protocol should be enabled, before executing this command. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent.

Example

```
Your Product(config-router)# nsf ietf restart-interval 300
plannedOnly
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf redist-config` – Displays the configuration information to be applied to the routes learnt from the RTM.

34.29 nsf ietf helper disable

Command Objective This command disables the helper support.

The no form of the command enables the helper support.

Syntax

```
nsf ietf helper disable [unknown] [softwareRestart]
[swReloadUpgrade] [switchToRedundant]

no nsf ietf helper disable [unknown][softwareRestart]
[swReloadUpgrade] [switchToRedundant]
```

Parameter Description

- `unknown` - Disables / enables helper support for restarting of system due to unplanned events (such as restarting after a crash).
- `softwareRestart` - Disables / enables helper support for restarting of `the` system due to restart of software.
- `swReloadUpgrade` - Disables / enables helper support for restarting of system due to reload or upgrade of software.
- `switchToRedundant` - Disables / enables helper support for restarting of system due to switchover to a redundant support processor.

Mode Router Configuration Mode

Default Helper support is enabled.

☞ OSPFv3 routing protocol should be enabled, before executing this command.

Example

```
Your Product(config-router)# nsf ietf helper disable
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `nsf ietf helper gracetimelimit` - Configures the helper grace time limit
- `show ipv6 ospf redist-config` – Displays the configuration information to be applied to the routes learnt from the RTM.

34.30 nsf ietf helper gracetimelimit

Command Objective

This command configures the grace period till which the 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 1 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 configures the helper grace time limit as zero.

Syntax

```
nsf ietf helper gracetimelimit <gracelimit period(1-1800)>
no nsf ietf helper gracetimelimit
```

Mode

Router Configuration Mode

Default

0

☞ OSPFv3 routing protocol and OSPFv3 helper support should be enabled, before configuring the helper grace time limit.

Example

```
Your Product(config-router)# nsf ietf helper
gracetimelimit 150
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `no nsf ietf helper disable` - Enables the helper support.
- `show ipv6 ospf neighbor` – Displays OSPFv3 neighbors information.

34.31 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 helper Mode, once topology change is detected during the graceful restart process.

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

Router Configuration Mode

Default

Strict LSA check option is disabled in helper.

☞ OSPFv3 routing protocol and OSPFv3 helper support should be enabled, before enabling the strict LSA check option in the helper.

Example

```
Your Product(config-router)# nsf ietf helper strict-lsa-checking
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `no nsf ietf helper disable` - Enables the helper support.
- `show ipv6 ospf - General Information` – Displays general information about the OSPFv3 routing process.

34.32 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 no form of the command disables the Grace Ack Required state in restarter.

Syntax

```
nsf ietf grace lsa ack required
no nsf ietf grace lsa ack required
```

Mode Router Configuration Mode

Default Grace Ack Required state is enabled in restarter.

☞ OSPFv3 routing protocol should be enabled, before executing this Command. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent.

Example

```
Your Product(config-router)# no nsf ietf grace lsa ack required
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.

34.33 nsf ietf grace lsa retransmit-count

Command Objective

This command configures the maximum number of retransmissions for unacknowledged GraceLSA. This value specifies the number of retransmissions of unacknowledged GraceLSAs. This value ranges between 0 and 180.

The no form of the command resets the GraceLSA retransmission count to default value.

Syntax

```
nsf ietf grace lsa retransmit-count <retransmit-count (0-180)>

no nsf ietf grace lsa retransmit-count
```

Mode

Router Configuration Mode

Default

2

☞ OSPFv3 routing protocol should be enabled, before executing this command.

Example

```
Your Product(config-router)# nsf ietf grace lsa retransmit-count 100
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.

34.34 nsf ietf restart-reason

Command Objective This command configures the reason for restart.

Syntax `nsf ietf restart-reason {unknown | softwareRestart | swReloadUpgrade | switchToRedundant}`

Parameter Description

- `unknown` - Sets the system to restart due to unplanned events (such as restarting after a crash).
- `softwareRestart` - Sets the system to restart due to restart of software.
- `swReloadUpgrade` - Sets the system to restart due to reload or upgrade of software.
- `switchToRedundant` - Sets the system to restart due to switchover to a redundant support processor.

Mode Router Configuration Mode

Default unknown.

☞ OSPFv3 routing protocol should be enabled, before executing this command. The entity should save any change made using this command in a non-volatile storage, as the configuration set using this command is persistent.

Example

```
Your Product(config-router)# nsf ietf restart-reason
softwareRestart
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.

34.35 ipv6 ospf area

Command Objective

This command enables OSPFv3 for IPv6 on an interface.

The no form of the command disables OSPFv3 routing protocol on the interface and triggers a flushing of the self-originated Link Scope LSAs, and deletes the Link Scope LSAs associated with this interface from the Link State Database. If there is a single interface in the associated area, then this command deletes its Area Scope LSAs from the Link State Database.

Syntax

```
ipv6 ospf area <IPv4-Address> [instance <instance-id>]
no ipv6 ospf
```

Parameter Description

- `<IPv4-Address>` - Configures an IPv4 address to enable the OSPFv3.
- `instance <instance-id>` - Configures an ID of the OSPFv3 instance to be run over a link. This ID has local link significance only.

Mode

Interface configuration Mode (VLAN interface / Router port)

Default

- OSPv3 routing protocol is disabled.
- instance-id - 0

☞ This command executes only if OSPFv3 is enabled. The router id is set for the router.

Example

```
Your Product(config-if)# ipv6 ospf area      0.0.0.0
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `router-id`– Sets the router-id for the router.
- `show ipv6 ospf - General Information` – Displays general information about the OSPFv3 routing process.
- `show ipv6 ospf interface` – Displays the OSPFv3-related interface information.
- `show ipv6 ospf - request/retrans-list` - Displays the list of all link state advertisements (LSAs) in request-list or in retransmission-list.

34.36 ipv6 ospf demand-circuit

Command Objective

This command configures OSPFv3 to treat the interface as an OSPFv3 demand circuit. It indicates whether Demand OSPFv3 procedures (hello suppression to FULL neighbors and setting the DoNotAge flag on propagated LSAs) must be performed on the configured interface.

The no form of the command disables the demand circuit on an interface.

Syntax

```
ipv6 ospf demand-circuit
no ipv6 ospf demand-circuit
```

Mode

Interface configuration Mode (VLAN interface / Router port)

Default

Disabled

☞ This command executes only if OSPFv3 is enabled. The routing support for demand routing must have been enabled (using the demand-extensions command) prior to the execution of this command.

Example

```
Your Product(config-if)# ipv6 ospf demand-circuit
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `ipv6 ospf neighbor probing` - Enables neighbor probing on demand-circuit enabled interface.
- `demand-extensions` – Enables routing support for demand routing.
- `show ipv6 ospf interface` – Displays the OSPFv3-related interface information.

34.37 ipv6 ospf retransmit-interval

Command Objective

This command sets the time between LSA retransmissions for adjacencies belonging to interface. This value ranges between 1 and 1800 The retransmit time interval is the number of seconds between the link-state advertisement retransmissions for adjacencies belonging to an interface. The retransmit-interval value is also used while retransmitting database description and link-state request packets.

The no form of the command resets the retransmit interval for an interface to its default value.

Syntax

```
ipv6 ospf retransmit-interval <interval>
no ipv6 ospf retransmit-interval
```

Mode

Interface configuration Mode (VLAN interface / Router port)

Default

interval - 5

This command executes only if OSPFv3 is enabled.

Example

```
Your Product(config-if)# ipv6 ospf retransmit-interval 10
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf interface` – Displays the OSPFv3-related interface information.

34.38 ipv6 ospf transmit-delay

Command Objective

This command sets the estimated time taken to transmit LS update packet over a particular interface. This delay value ranges between 1 and 1800.

The no form of the command sets the default transmit delay for an interface.

Syntax

```
ipv6 ospf transmit-delay <delay>

no ipv6 ospf transmit-delay
```

Mode

Interface configuration Mode (VLAN interface / Router port)

Default

delay - 1

☞ This command executes only if OSPFv3 is enabled.

Example

```
Your Product(config-if)# ipv6 ospf transmit-delay 10
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf interface` – Displays the OSPFv3-related interface information.

34.39 ipv6 ospf priority

Command Objective

This command sets the router priority, which helps to determine the Designated Router for this network. This value ranges between 1 and 255.

The no form of the command sets the default router priority for an interface.

Syntax

```
ipv6 ospf priority < priority (1-255)>

no ipv6 ospf priority
```

Mode

Interface configuration Mode (VLAN interface / Router port)

Default

priority - 1

☞ This command executes only if OSPFv3 is enabled.

Example

```
Your Product(config-if)# ipv6 ospf priority 7
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf interface` – Displays the OSPFv3-related interface information.

34.40 ipv6 ospf hello-interval

Command Objective

This command specifies the time interval between the OSPFv3 hello packets on a particular interface (the length of time, in seconds, between the Hello packets that the router sends on the interface).

The no form of the command sets the default hello interval for an interface.

Syntax

```
ipv6 ospf hello-interval <1-65535>
no ipv6 ospf hello-interval
```

Mode

Interface configuration Mode (VLAN interface / Router port)

Default

interval - 10

☞ This command executes only if OSPFv3 is enabled. The hello interval value must be same for all routers attached to a common link.

Example

```
Your Product(config-if)# ipv6 ospf hello-interval 20
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf interface` – Displays the OSPFv3-related interface information.

34.41 ipv6 ospf dead-interval

Command Objective

This command configures the router dead interval. It is configured in seconds and indicates the time period for which the router waits for hello packet from the neighbor before declaring this neighbor down.

The no form of the command sets the interface dead interval to default value.

Syntax

```
ipv6 ospf dead-interval <1-65535>
no ipv6 ospf dead-interval
```

Mode

Interface configuration Mode (VLAN interface / Router port)

Default

interval - 40

☞ This command executes only if OSPFv3 is enabled. This value must be a multiple of the Hello interval and must be same for all routers attached to a common link.

Example

```
Your Product(config-if)# ipv6 ospf dead-interval 50
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf interface` – Displays the OSPFv3-related interface information.

34.42 ipv6 ospf poll-interval

Command Objective

This command configures the larger time interval, in seconds, between the Hello packets sent to an inactive non-broadcast multi-access neighbor.

The no form of the command sets the default poll interval for an interface.

Syntax

```
ipv6 ospf poll-interval <interval>

no ipv6 ospf poll-interval
```

Mode

Interface configuration Mode (VLAN interface / Router port)

Default

interval - 120

☞ This command executes only if OSPFv3 is enabled.

Example

```
Your Product(config-if)# ipv6 ospf poll-interval 30
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf interface` – Displays the OSPFv3-related interface information.

34.43 ipv6 ospf metric

Command Objective

This command explicitly specifies the metric value for sending a packet on an interface. This value ranges between 1 and 65535.

The no form of the command sets the default value for the interface metric.

Syntax

```
ipv6 ospf metric <metric>

no ipv6 ospf metric
```

Mode

Interface configuration Mode (VLAN interface / Router port)

Default

metric - Reference Bandwidth / ifSpeed

☞ This command executes only if OSPFv3 is enabled.

Example

```
Your Product(config-if)# ipv6 ospf metric 20
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf interface` – Displays the OSPFv3-related interface information.

34.44 ipv6 ospf network

Command Objective This command sets the network type for an interface.

The no form of the command sets the default value for the network type.

Syntax

```
ipv6 ospf network { broadcast | non-broadcast | point-to-multipoint | point-to-point }

no ipv6 ospf network
```

Parameter Description

- `broadcast` - Configures a network that supports 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 a network that supports many (more than
- two) routers, but having no broadcast capability.
- `point-to-multipoint` - Treats the non-broadcast network as a collection of point-to-point links.
- `point-to-point` - Configures a network that joins a single pair of routers.

Mode Interface configuration Mode (VLAN interface / Router port)

Default broadcast

☞ This command executes only if OSPFv3 is enabled. If the Interface Network type is NBMA or Point-to-Multipoint, neighbor must be configured. When there are few configured neighbors on the interface, then both network type change command and the no form of the command do not succeed.

Example

```
Your Product(config-if)# ipv6 ospf network non-broadcast
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `ipv6 ospf neighbor` – Configures a neighbor on non-broadcast networks.
- `show ipv6 ospf interface` – Displays the OSPFv3-related interface information.
- `ipv6 ospf linkLSASuppress` – Configures the interface to suppress Link LSA origination.

34.45 ipv6 ospf neighbor

Command Objective

This command configures a neighbor on non-broadcast networks and sets the priority value for the neighbor if specified.

The no form of the command deletes a configured neighbor or sets the default priority value (if the priority option is specified).

Syntax

```
ipv6 ospf neighbor <IPv6-Address> [priority <1-255>]
no ipv6 ospf neighbor <IPv6-Address> [priority]
```

Parameter Description

- `<IPv6-Address>` - IPv6 Address Prefix.
- `priority <1-255>` - A number that specifies the router priority.

Mode

Interface configuration Mode (VLAN interface / Router port)

Default

priority – 1

☞ This command executes only if OSPFv3 is enabled. In the OSPFv3 protocol packets, the IPv6 address indicates the source address of the neighbor. The Link Local address of the neighbor must be used for this field. Neighbors can be configured only in NBMA networks and Point-to-Multipoint networks.

Example

```
Your Product(config-if)# ipv6 ospf neighbor
fe80::220:35ff:fe43:6020 priority 2
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf interface` – Displays the OSPFv3-related interface information.
- `show ipv6 ospf neighbor` – Displays OSPFv3 neighbors information.

34.46 ipv6 ospf passive-interface

Command Objective

This command configures an OSPFv3 interface to be Passive. The execution of the command results in suppressing OSPFv3 protocol packets traffic on this interface.

The no form of the command configures an OSPFv3 interface to be non-passive.

Syntax

```
ipv6 ospf passive-interface
no ipv6 ospf passive-interface
```

Mode

Interface configuration Mode (VLAN interface / Router port)

Default

Disabled

☞ This command executes only if OSPFv3 is enabled.

Example

```
Your Product(config-if)# ipv6 ospf passive-interface
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `show ipv6 ospf interface` – Displays the OSPFv3-related interface information.

34.47 ipv6 ospf neighbor probing

Command Objective

This command enables neighbor probing on demand-circuit enabled interface.

The no form of the command disables neighbor probing on demand-circuit enabled interface.

Syntax

```
ipv6 ospf neighbor probing
no ipv6 ospf neighbor probing
```

Mode

Interface configuration Mode (VLAN interface / Router port)

Default

Disabled

☞ This command executes only if OSPFv3 is enabled and the Demand Extension feature is enabled.

Example

```
Your Product(config-if)# ipv6 ospf neighbor probing
```

Related Command(s)

- `show ipv6 ospf interface` – Displays the OSPFv3-related interface Iinformation.
- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `ipv6 ospf demand-circuit` - Configures OSPFv3 to treat the interface as an OSPFv3 demand circuit

---

34.48 ipv6 ospf neighbor-probe retransmit-limit

Command Objective	This command sets the number of consecutive LSA retransmissions before the neighbor is deemed inactive. This value ranges between 0 and 999999999. The no form of the command sets the default neighbor probe retransmission limit.

Syntax	`ipv6 ospf neighbor-probe retransmit-limit <retrans-limit>`
	
	`no ipv6 ospf neighbor-probe retransmit-limit`

Mode	Interface configuration Mode (VLAN interface / Router port)
Default	retrans-limit - 10
	☞ This command executes only if OSPFv3 is enabled. Demand Extension feature is enabled.
Example	`Your Product(config-if)# ipv6 ospf neighbor-probe retransmit-limit 30`

Related Command(s)

- `show ipv6 ospf interface` – Displays the OSPFv3-related interface information.
- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `ipv6 ospf demand-circuit` - Configures OSPFv3 to treat the interface as an OSPFv3 demand circuit

34.49 ipv6 ospf neighbor-probe interval

Command Objective

This command sets the number of seconds, that indicates how often neighbor will be probed.

The no form of the command sets the default neighbor probe interval. This value ranges between 0 and 999999999.

Syntax

```
ipv6 ospf neighbor-probe interval <interval>
no ipv6 ospf neighbor-probe interval
```

Mode

Interface configuration Mode (VLAN interface / Router port)

Default

interval - 120

☞ This command executes only if OSPFv3 is enabled. Demand Extension feature is enabled.

Example

```
Your Product(config-if)# ipv6 ospf neighbor-probe interval
200
```

Related Command(s)

- `show ipv6 ospf interface` – Displays the OSPFv3-related interface information.
- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `ipv6 ospf demand-circuit` - Configures OSPFv3 to treat the interface as an OSPFv3 demand circuit.

34.50 debug ipv6 ospf - pkt

Command Objective This command sets the trace levels.

The no form of the command resets the trace levels.

Syntax

```
debug ipv6 ospf [vrf <contextname>] [pkt ( [{high | low |
hex}] [hp] [ddp] [lrq] [lsu] [lsa] )] [level ([fn_entry]
[fn_exit] [critical] [mem_alloc_succ] [mem_alloc_fail])]
[module ( [ppp] [rtm] [nssa] [rt_aggrg] [adj_formation]
[lsdb] [ism] [nsm] [rt_calc] [interface] [config]
[restarting-router] [helper] [redundancy])]
```

```
no debug ipv6 ospf [vrf <contextname>] [ pkt ( [{high |
low | hex}] [hp] [ddp] [lrq] [lsu] [lsa] )] [level
( [fn_entry] [fn_exit] [critical] [mem_alloc_succ]
[mem_alloc_fail] )] [ module ( [ppp] [rtm] [nssa]
[rt_aggrg] [adj_formation] [lsdb] [ism] [nsm] [rt_calc]
[interface] [config] [restarting-router] [helper]
[redundancy]) ]
```

Parameter Description

- `vrf<contextname>` - Sets the trace level for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
- `pkt` - Sets the trace level of packet High Level Dump debug messages.
- `high` - Packet High Level Dump Trace.
- `low` - Packet Low Level Dump Trace.
- `hex` - Packet Hex 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.
- `level` - Generates debug statements for the following:
- `fn_entry` - Function Entry trace
- `fn_exit` - Function Exit trace
- `critical` - Generates debug statements for OSPF critical traces. These traces are used for cases such as failure of RBTree addition, failure to program the hardware, and so on.
- `mem_alloc_succ` - Memory Allocation Success trace.
- `mem_alloc_fail` - Memory Allocation Failure trace.
- `module` - OSPFv3 Module Debug Messages.
- `ppp` - Protocol Packet Processing Trace.
- `rtm` - RTM Module Trace.
- `nssa` - NSSA Trace.

- **rt_aggrg** - Route Aggregation Trace.
- **adj_formation** - Adjacency Formation Trace.
- **lsdb** - Link State Database Trace.
- **ism** - Interface State Machine Trace.
- **nsm** - Neighbor State Machine Trace.
- **rt_calc** - Routing Table Calculation Trace.
- **interface** - Interface Trace.
- **config** - Configuration Trace.
- **restarting-router** - Debug messages related to restarting router.
- **helper** - Debug messages related to router in helper Mode.
- **redundancy** - High redundancy trace.

Mode	Privileged EXEC Mode
Default	Debugging is disabled.
Example	**Your Product# debug ipv6 ospf pkt high hp level fn_entry module ppp**

Related Command(s)

- **ip vrf** - Creates VRF instance.
- **ipv6 router ospf** - Enables the OSPFv3 routing protocol.
- **show ipv6 ospf - General Information** – Displays general information about the OSPFv3 routing process.

34.51 show ipv6 ospf - interface

Command Objective This command displays the general configured information of OSPFv3 for the specified interface.

Syntax

```
show ipv6 ospf [vrf <contextname>] interface [ vlan <vlan-id(1-4094)> ]
```

Parameter Description

- **vrf<context name>** - Displays general OSPFv3 information for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string of size 32.
- **vlan<vlan-id(1-4094)>** - Displays general OSPFv3 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

Default vlan - 1

Example

```
Your Product# show ipv6 ospf interface
Ospfv3 Interface Information
Interface Name: vlan1  Interface Id: 33  Area Id: 0.0.0.0
Local Address: fe80::202:2ff:fe03:401  Router Id: 0.0.0.0
Network Type: PTOP  Cost: 1  State: PTOP
Designated Router Id: 0.0.0.0 local address: (null)
Backup Designated Router Id: 0.0.0.0 local address: (null)
Transmit Delay: 1 sec  Priority: 1  IfOptions: 0x0
Timer intervals configured:
Hello: 10, Dead: 40, Retransmit: 5, Poll: 120
Demand Circuit: Disable Neighbor Probing:
Disable Link Lsa Suppression: Enable
Nbr Probe Retrans Limit: 10   Nbr Probe Interval: 120
Hello due in 6 sec
Neighbor Count is: 0
```

Related Command(s)

- `area - virtual-link` – Sets the Virtual Link between Areas.
- `ipv6 ospf area` – Enables OSPFv3 for IPv6 on an interface.
- `ipv6 ospf demand-circuit` – Configures OSPFv3 to treat the interface as an OSPFV3 demand circuit.
- `ipv6 ospf retransmit-interval` – Sets the time between LSA retransmissions for adjacencies belonging to an interface.
- `ipv6 ospf transmit-delay` – Sets the estimated time taken to transmit LS update packet over a particular interface.
- `ipv6 ospf priority` – Sets the router priority, which helps to determine the Designated Router for this network.
- `ipv6 ospf hello-interval` – Specifies the time interval between the OSPFv3 hello packets on a particular interface.
- `ipv6 ospf dead-interval` – Configures the router dead interval.
- `ipv6 ospf poll-interval` – Configures the larger time interval, in seconds, between the Hello packets sent to an inactive non-broadcast multi-access neighbor.
- `ipv6 ospf metric` – Specifies the metric value for sending a packet on an interface.
- `ipv6 ospf network` – Sets the network type for an interface.
- `ipv6 ospf neighbor` – Configures a neighbor on non-broadcast networks and sets the priority value for the neighbor if specified.
- `ipv6 ospf passive-interface` – Configures an OSPFv3 interface to be Passive.
- `ipv6 ospf neighbor probing` – Enables neighbor probing on demand-circuit enabled interface.
- `ipv6 ospf neighbor-probe retransmit-limit` – Sets the number of consecutive LSA retransmissions before the neighbor is deemed inactive.
- `ipv6 ospf neighbor-probe interval` – Sets the number of seconds, that indicates how often neighbor will be probed.
- `ipv6 ospf linkLSASuppress` – Configures the interface to suppress Link LSA origination.

34.52 show ipv6 ospf - neighbor

Command Objective This command displays OSPFv3 neighbor information.

Syntax

```
show ipv6 ospf [vrf <contextname>] neighbor [ <Neighbor-RouterID> ]
```

Parameter Description

- `vrf <contextname>` - Displays OSPFv3 neighbor information for the specified VRF instance. This value represents unique name of the VRF instance.
- `<Neighbor-RouterID>` - Displays the OSPFv3 information for the specified router ID. This value ranges between 0 and 64.

Mode Privileged EXEC Mode

Example

```
Your Product# show ipv6 ospf neighbor
ID        Pri   State     DeadTime Address       Helper     HelperAge HelperExitReason
20.0.0.3  1     FULL/BACKUP  35    fe80::203:2ff:fe03:401  Not Helping  0     0
```

Related Command(s)

- `ipv6 ospf neighbor` – Configures a neighbor on non-broadcast networks and sets the priority value for the neighbor if specified.
- `nsf ietf helper gracetimelimit` - Configures the helper grace time limit.

34.53 show ipv6 ospf - request/retrans-list

Command Objective This command displays the list of all link state advertisements (LSAs) in request-list or in retransmission-list.

Syntax

```
show ipv6 ospf [vrf <contextname>] { request-list |
retrans-list } [ <Neighbor-RouterID> ]
```

Parameter Description

- **vrf <contextname>** - Displays the LSAs in request-list or in retransmission-list for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
- **request-list** - Displays the list of Link State Advertisements for which the neighbor has more up-to-date instances.
- **retrans-list -** Displays the list of Link State Advertisements that have been sent but not acknowledged.
- **<Neighbor-RouterID>** - Displays the list of all link state advertisements (LSAs) in request-list or in retransmission-list for the specified neighbor router ID.

Mode Privileged EXEC Mode

Example

```
Your Product# show ipv6 ospf retrans-list 1.0.0.1
    Vrf    switch1
    NeighborId: 11.0.0.2   Nbr Address:
    fe80::211:22ff:fe33:4422
    Type   LsId        AdvRtr     SeqNo       Age
    Checksum
    0x2009 11.0.0.1    11.0.0.1   0x3000080   0
    0xc7f5
    Vrf    switch2
    NeighborId: 11.0.0.1   Nbr Address:
    fe80::211:22ff:fe33:4421
    Type   LsId        AdvRtr     SeqNo       Age
    Checksum
    0x2001 11.0.0.2    11.0.0.2   0x2000080   0
```

```
                    0xebf3
```

Related Command(s)

- `ipv6 router ospf` - Enables the OSPFv3 routing protocol.
- `router-id` – Sets the router-id for the router.
- `ipv6 ospf area` – Enables OSPFv3 for IPv6 on an interface.

34.54 show ipv6 ospf virtual-links

Command Objective This command displays the parameters and the current state of OSPFv3 virtual links.

Syntax `show ipv6 ospf [vrf <contextname>] virtual-links`

Parameter Description

- `vrf <contextname>` - Displaysthe parameters and the current state of OSPFv3 virtual links 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 User/Privileged EXEC Mode

Example

```
Your Product# show ipv6 ospf virtual-links

    Vrf switch3

    Interface State: DOWN, Neighbor State: DOWN Transit Area:
    0.0.0.2, Virtual Neighbor: 11.0.0.8 Intervals Configured for
    the Virtual Interface: Hello: 10, Dead: 60, Transit: 1,
    Retransmit : 5
```

Related Command(s)

- `area - virtual-link` – Sets the Virtual Link between Areas.

34.55 show ipv6 ospf border-routers

Command Objective This command displays the internal OSPFv3 routing table entries to an ABR/ASBR.

Syntax `show ipv6 ospf [vrf <contextname>] border-routers`

Parameter Description

- `vrf <contextname>` - Displays the internal OSPFv3 routing table entries 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 ipv6 ospf border-routers
OSPFv3 Process Border Router Information
Destination Type  NextHop                 Cost  Rt Type       Area Id
10.10.10.1  ASBR  fe80::230:48ff:fee3:475 200  intraArea     0.0.0.0
```

Related Command(s)

- `abr-type` – Sets the ABR (Area Border Router) type.
- `ASBR Router` – Configures the router as an ASBR.

34.56 show ipv6 ospf - area-range / summary-prefix

Command Objective This command displays either the list of all area address ranges information or all external summary address configuration information.

Syntax `show ipv6 ospf [vrf <contextname>] { area-range | summary-prefix }`

Parameter Description

- `vrf <contextname>` - Displaysthe area address ranges for the specified VRF instance. This value represents unique name of the VRF instance. This value is a string whose maximum size is 32.
- `area-range` - Displays the area associated with the OSPFv3 address range.
- `summary-prefix` - Displays the aggregate addresses for OSPFv3.

Mode User/Privileged EXEC Mode

Example

```
Your Product# show ipv6 ospf area-range
Ospfv3 Summary Address Configuration Information
Vrf switch8
Network        PfxLength    LSA Type    Area    Effect    Tag
3ffe:801:481d::  48        Summary     0.0.0.0 advertise  0
Your Product# show ipv6 ospf summary-prefix
Ospfv3 External Summary AddressConfiguration Information
Vrf switch3
Prefix  PfxLength  AreaId  Effect  TranslationState
3ffe::172:100:0:0  88    0.0.0.1     advertise   enabled
3ffe::172:200:0:0  88    0.0.0.4     advertise   enabled
```

Related Command(s)

- `area - range` – Creates the Internal Aggregation Address Range.
- `area – summary-prefix` – Enables route aggregation/filtering while importing routes in the OSPFv3 domain.
- `no area` - Deletes an area.

34.57 show ipv6 ospf - General Information

Command Objective This command displays general information about OSPFv3 routing process.

Syntax `show ipv6 ospf [vrf <contextname>]`

Parameter Description

- `vrf <contextname>` - Displays general information about OSPFv3 routing process 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 ipv6 ospf
Router Id: 20.0.0.2   ABR Type:  Standard ABR
SPF schedule delay: 5 secs Hold time between two SPFs: 10
secs
Exit Overflow Interval: 0 Ref BW: 100000   Ext Lsdb Limit:
-1
Trace Value: 0x00000800     As Scope Lsa: 0 Checksum Sum:
0x0
Demand Circuit: Enable
Passive Interface: Disable
Nssa Asbr default Route Translation: Disable
Autonomous System Boundary Router Number of Areas in this
router 1
Route calculation staggering is enabled
Route calculation staggering interval is 10 seconds IETF
Non-Stop Forwarding enabled
Restart-interval limit: 100 sec
Restart exit reason: none
IETF NSF helper support enabled Area 0.0.0.0
Number of interfaces in this area is   1
Number of Area Scope Lsa: 4 Checksum Sum: 0x257bb
```

```
Number of Indication Lsa: 0 SPF algorithm executed: 2
times
```

Related Command(s)

- **router-id** - IPv4-Address – Sets a fixed router ID.
- **timers spf** – Configures the delay time and the hold time between two consecutive SPF calculations.
- **abr-type** – Sets the ABR (Area Border Router) type.
- **ASBR Router** – Configures the router as an ASBR.
- **passive-interface** – Sets the global default passive interface status.
- **route-calculation staggering** - Enables OSPFv3 route calculation Staggering.
- **route-calculation staggering-interval** - Configures the OSPFv3 route calculation staggering interval.
- **nssaAsbrDfRtTrans** – Enables setting of P bit in the default Type-7 LSA generated by an NSSA internal ASBR.
- **as-external lsdb-limit** – Sets the maximum number of non-Default AS-external-LSAs entries that can be stored in the link-state database.
- **exit-overflow-interval** – Sets the number of seconds after which a router will attempt to leave the Overflow State.
- **demand-extensions** – Enables routing support for demand routing.
- **reference-bandwidth** – Sets the reference bandwidth in kilobits per and configures grace interval.
- **nsf ietf restart-interval** - Enables the graceful restart support AS-external-LSAs entries that can be stored in the link-state database.
- **nsf ietf helper disable** - Disables the helper support.
- **nsf ietf helper strict-lsa-checking** - Enables the strict LSA check option in helper.
- **ipv6 ospf area** – Enables OSPFv3 for IPv6 on an interface.
- **debug ipv6 ospf -pkt** – Sets the trace levels.

34.58 show ipv6 ospf - LSA Database

Command Objective This command displays the LSA information.

Syntax

```
show ipv6 ospf [vrf <contextname>] [area <AreaID>]
database [{router|network|as-external|inter-prefix|inter-
router|intra-prefix|link|nssa}] [{detail|HEX}]
```

Parameter Description

- **vrf <contextname>** - Displays the LSA information for the specified VRF instance. This value represents unique name of the VRF instance.
- **area<AreaID>** - Displays the LSA information for the specified area.
- **database** - Displays the number of each type of LSA for each area in the database.
- **router** - Displays the LSA information for the specified Router LSAs.
- **as-external** - Displays the LSA information for the specified AS-External LSAs.
- **inter-prefix** - Displays the LSA information for the specified Inter-prefix LSAs.
- **intra-prefix** - Displays the LSA information for the specified Intra-prefix LSAs.
- **link** - Displays the LSA information for the specified Link State LSAs.
- **nssa** - Displays the LSA information for the specified NSSA LSAs.
- **detail** - Displays the LSAs information in detail.
- **HEX** - Displays the LSAs information in hexadecimal format.

Mode Privileged EXEC Mode

Example

```
Your Product# show ipv6 ospf database
Vrf            switch1
AreaId   RtrId       LsaType     Age    Seq#       Checksum
0.0.0.1  11.0.0.1    0x0008      0      0x80000002  0xe9d0
0.0.0.1  11.0.0.2    0x0008      8      0x80000002  0xe5d0
0.0.0.1  11.0.0.1    0x2001      0      0x80000001  0x23bc
0.0.0.1  11.0.0.2    0x2001      8      0x80000003  0x4d6
Vrf      switch2
```

AreaId	RtrId	LsaType	Age	Seq#	Checksum
0.0.0.1	11.0.0.1	0x0008	9	0x80000002	0xe9d0
0.0.0.1	11.0.0.2	0x0008	0	0x80000002	0xe5d0
3.3.3.3	11.0.0.2	0x0008	0	0x80000002	0x613e
0.0.0.1	11.0.0.1	0x2001	3	0x80000001	0x23bc
0.0.0.1	11.0.0.2	0x2001	0	0x80000003	0x4d6
3.3.3.3	11.0.0.2	0x2001	0	0x80000001	0xac4f
3.3.3.3	11.0.0.2	0x2007	0	0x80000002	0x428

Vrf switch3

AreaId	RtrId	LsaType	Age	Seq#	Checksum
3.3.3.3	11.0.0.3	0x0008	0	0x80000002	0x6a6
3.3.3.3	11.0.0.3	0x0008	0	0x80000002	0x5d3e
3.3.3.3	11.0.0.3	0x0008	0	0x80000002	0xb4d5
3.3.3.3	11.0.0.7	0x0008	8	0x80000002	0x5e15
3.3.3.3	11.0.0.3	0x0008	0	0x80000002	0xc6d
3.3.3.3	11.0.0.7	0x0008	8	0x80000002	0xb5ac
3.3.3.3	11.0.0.3	0x2001	0	0x80000002	0xf07c
3.3.3.3	11.0.0.7	0x2001	3	0x80000002	0x6f02

34.59 show ipv6 ospf - route

Command Objective This command displays routes learned by the OSPFv3 process.

Syntax `show ipv6 ospf [vrf <contextname>] route`

Parameter Description

- `vrf <contextname>` - Displays the routes learnt by the OSPFv3 process for the specified VRF instance. This value represents unique name of the VRF instance.

Mode Privileged EXEC Mode

Example

```
Your Product# show ipv6 ospf route
OSPFV3 Process Routing Table
Vrf switch3
Dest/Prefix-Length  NextHop/IfIndex    Cost  Rt.Type  Area
::/0  fe80::211:22ff:fe33:4432 /Slot0/6  3   type1Ext 3.3.3.3
Vrf switch7
Dest/Prefix-Length  NextHop/IfIndex    Cost  Rt.Type  Area
::/0  fe80::211:22ff:fe33:4443 /Slot0/23  7  type1Ext 3.3.3.3
Vrf switch8
Dest/Prefix-Length  NextHop/IfIndex    Cost  Rt.Type  Area
::/0  fe80::211:22ff:fe33:4426 /Slot0/26  9  type1Ext 3.3.3.3
```

Related Command(s)

- `ipv6 router ospf` – Enables the OSPFv3 routing protocol.
- `router-id` - IPv4-Address – Sets a fixed router ID.

34.60 show ipv6 ospf - areas

Command Objective This command displays the Area Table.

Syntax `show ipv6 ospf [vrf <contextname>] areas`

Parameter Description

- `vrf <contextname>` - Displays area table information for the specified VRF instance. This value represents unique name of the VRF instance.

Mode Privileged EXEC Mode

Example

```
Your Product# show ipv6 ospf areas
AreaId: 0.0.0.0                 Area Type: NORMAL AREA
Spf Calculation: 0 (times)      Area Bdr Rtr Count: 0
As Bdr Rtr Count: 0             Area Summary: Send Summary
  Vrf  default

AreaId: 2.2.2.2                 Area Type: NORMAL AREA
Spf Calculation: 0 (times)      Area Bdr Rtr Count: 0
As Bdr Rtr Count: 0             Area Summary: Send Summary
  Vrf  default

AreaId: 10.1.1.1                Area Type: NORMAL AREA
Spf Calculation: 0 (times)      Area Bdr Rtr Count: 0
As Bdr Rtr Count: 0             Area Summary: Send Summary
```

Related Command(s)

- `area - stub/nssa` – Defines an area as a stub area or an NSSA (Not So Stubby Area).
- `area - stability-interval` – Configures the stability interval (in seconds) for the NSSA.
- `area - translation-role` – Configures the translation role for NSSA.
- `no area` – Deletes an area.

34.61 show ipv6 ospf - host

Command Objective This command displays the Host Table information.

Syntax `show ipv6 ospf [vrf <contextname>] host`

Parameter Description

- `vrf <contextname>` - Displays host table information for the specified VRF instance. This value represents unique name of the VRF instance.

Mode Privileged EXEC Mode

Example

```
Your Product# show ipv6 ospf host
        OSPFV3 HOST CONFIGURATION Information
        Address                 AreaId    StubMetric
        Vrf switch1
        3ffe:501:481d:f001::1 0.0.0.1     10
        Vrf switch1
        3ffe:601:481d:f001::1 0.0.0.1     10
        Vrf switch5
        3ffe:501:481d:f004::5 0.0.0.0     10
        Vrf switch6
        3ffe:501:481d:f004::6 0.0.0.0     10
```

Related Command(s)

- `host - metric/area-id` – Configures a host entry with metric and/or area-id.

34.62 show ipv6 ospf - redist-config

Command Objective This command displays the configuration information to be applied to the routes learnt from the RTM.

Syntax `show ipv6 ospf [vrf <contextname>] redist-config`

Parameter Description

- `vrf <contextname>` - Displays the information for the specified VRF instance. This value represents unique name of the VRF instance.

Mode Privileged EXEC Mode

Example

```
Your Product# show ipv6 ospf redist-config

Ospfv3 External Summary AddressConfiguration Information

Vrf switch3

Address Prefix PfxLength MetricType Metric TagType TagValue

3ffe::100:100:0:0 88 asExtType1 10 manual 0

3ffe::100:200:0:0 88 asExtType1 20 manual 0

3ffe::100:300:0:0 88 asExtType1 30 manual 0
```

Related Command(s)

- `redist-config` – Configures the information to be applied to routes learnt from RTM.

34.63 show ipv6 ospf redundancy

Command Objective This command displays OSPFv3 redundancy information.

Syntax `show ipv6 ospf redundancy`

Mode Privileged EXEC Mode

Example

```
Your Product# show ipv6 ospf redundancy
OSPFv3 Hot Standby Admin Status : Enabled
OSPFv3 Hot Standby State    : Active - Standby Up
OSPFv3 Hot Standby Dynamic Bulk Update Status :
Completed
OSPFv3      Hot Standby Hello Sync count     :     0
OSPFv3      Hot Standby LSA Sync count  :     0
```

34.64 ipv6 ospf linkLSASuppress

Command Objective

This command sets the number of seconds, that indicates how often neighbor will be probed This command sets the number of seconds, that indicates how often neighbor will be probed.

The no form of the command allows generation of link-LSA for the specified link.

Syntax

```
ipv6 ospf linkLSASuppress
no ipv6 ospf linkLSASuppress
```

Mode

Interface configuration Mode (VLAN interface / Router port)

Default

Link-LSA suppression is disabled

☞ This command executes only if OSPFv3 is enabled. OSPF netwok type is set as either point-to-point or point-to-multipoint.

Example

```
Your Product(config-if)# ipv6 ospf linkLSASuppress
```

Related Command(s)

- `ipv6 router ospf` - Enables the OSPFv3 routing protocol.
- `ipv6 ospf network` – Configures the network type for an interface.
- `show ipv6 ospf interface` - Displays the OSPFv3-related interface information.

---

35 DHCPv6

DHCPv6 (Dynamic Host Configuration Protocol for IPv6) enables DHCP servers to pass configuration parameters such as IPv6 network addresses, to IPv6 nodes. It allows to automatically allocate reusable network addresses and provides additional configuration flexibility.

Aricent DHCPv6 has DHCPv6 client, DHCPv6 server and DHCPv6 relay functionalities. Aricent DHCPv6 runs as an application over IPv6 and uses SLI (Socket Layer Interface) to send or receive messages from the corresponding client or server.

35.1 DHCPv6 Client

The DHCPv6 client is a node that initiates requests on a link to obtain configuration parameters (such as list of available DNS (Domain Name Server) servers) from DHCPv6 servers. It transmits and receives DHCP messages using link-local address or addresses determined through other mechanisms.

The list of CLI commands for the configuration of DHCPv6 Client is as follows

- snmp-server enable traps ipv6 dhcp client
- ipv6 dhcp client port
- ipv6 dhcp client syslog
- ipv6 address dhcp
- ipv6 dhcp authentication client
- ipv6 dhcp client-id type
- ipv6 dhcp client-id interface
- ipv6 dhcp timer
- ipv6 dhcp client information refresh minimum
- debug ipv6 dhcp client
- clear ipv6 dhcp client statistics
- show ipv6 dhcp
- show ipv6 dhcp interface
- show ipv6 dhcp client statistics

35.1.1 snmp-server enable traps ipv6 dhcp client

Command Objective

This command enables the SNMP traps notification messages for DHCPv6 client. It enables all the traps, when executed without any option.

This command allows to enable multiple SNMP traps for the DHCPv6 client. That is, both the specified trap notifications can be enabled one after the other.

The no form of the command disables the SNMP traps for the DHCPv6 client. It sets the trap as none, when executed without any option.\

Syntax

```
snmp-server enable traps ipv6 dhcp client [invalid-pkt] [auth-fail]
```

```
no snmp-server enable traps ipv6 dhcp client [invalid-pkt] [auth-fail]
```

Parameter Description

- `invalid-pkt` - Enables or disables the transmission of invalid packet trap notification message. This trap notification message is generated, when the received reply message is invalid.
- `auth-fail` - Enables or disables the transmission of HMAC authentication fail trap notification. This trap notification is generated, when the received reply message contains the authentication TLV and digest calculated at the client side that does not match with the received digest value. The digest is calculated at the client side with the realm and key ID values.

Mode

Global Configuration mode

Default

SNMP traps are disabled for the DHCPv6 client

Example

```
Your Product(config)# snmp-server enable traps ipv6 dhcp client invalid-pkt
```

Related Command(s)

- `show ipv6 dhcp` – Displays the configuration information

35.1.2 ipv6 dhcp client port

Command Objective This command configures the listen or transmit UDP (User Datagram Protocol) ports which contains the UDP listen port number. The client provides the listen port number in UDP header of Information Request message. The client processes the received reply message only when the destination port number in UDP header is equal to Port value.

Syntax

```
ipv6 dhcp client port { listen <value (1-65535)> |
transmit <value(1-65535)>}
```

Parameter Description

- `listen<value (1-65535)>` - Configures that the UDP listen port number to be provided in UDP header of the information-request message. This value ranges between 1 and 65535.
- `transmit<value(1-65535)>` - Configures that the UDP (User Datagram Protocol) destination port number to be provided in UDP header of the information-request message. This value ranges between 1 and 65535.

Mode Global Configuration mode

Default

- listen – 546
- transmit - 547

☞ Client processes the received reply message, only when the destination port number in the UDP header is equal to the client listen port number.

Example

```
Your Product(config)# ipv6 dhcp client port listen 540
```

Related Command(s)

- `show ipv6 dhcp` – Displays the configuration information.

35.1.3 ipv6 dhcp client syslog

Command Objective This command enables or disables the syslog generation and transmission of syslog notification messages. The DHCPv6 client will generate the syslog messages only when syslog is set as enabled.

Syntax `ipv6 dhcp client syslog {enable | disable}`

Parameter Description

- `enable` - Enables the transmission of syslog notification messages. DHCPv6 client generates syslog messages.
- `disable` - Disables the transmission of syslog notification messages. DHCPv6 client does not generate any syslog messages.

Mode Global Configuration mode

Default disable

Example

```
Your Product(config)# ipv6 dhcp client syslog enable
```

Related Command(s)

- `show ipv6 dhcp` – Displays the configuration information.

35.1.4 ipv6 address dhcp

Command Objective

This command enables the DHCPv6 client functionality over the interface and requests for configuration information from the client.

The no form of the command disables the DHCPv6 client functionality over the interface.

Syntax

```
ipv6 address dhcp
no ipv6 address dhcp
```

Mode

Interface Configuration mode (Vlan Interface Mode / Router)

Default

DHCPv6 client functionality is disabled

Example

```
Your Product(config-if)# ipv6 address dhcp
```

Related Command(s)

- `no switchport` – Configures the port as router port
- `ipv6 dhcp authentication client`– Defines the domain, client identifier and the corresponding authentication MD5 keys used to authenticate the information-request message and validate reply message
- `ipv6 dhcp client-id type` – Configures the DUID type to be used for the client identifier
- `ipv6 dhcp client-id interface` – Configures the interface that is used in the formation of the DUID based on LLT or on LL
- `ipv6 dhcp timer` – Configures various timer parameters for a retransmission algorithm of the information-request message
- `ipv6 dhcp client information refresh minimum` – Sets the minimum refresh timer value for the information-request message for client
- `clear ipv6 dhcp client statistics` – Clears the DHCPv6 client statistics for the specified interface or all the interfaces
- `show ipv6 dhcp interface` – Displays the configuration information and the DHCPv6 information received from the server for client, relay and server interfaces
- `show ipv6 dhcp client statistics` – Displays the DHCPv6 client statistics

35.1.5 ipv6 dhcp authentication client

Command Objective This command defines the domain, client identifier and the corresponding authentication MD5 (Message Digest 5) keys used to authenticate the information-request message and validate reply message.

Syntax `ipv6 dhcp authentication client {realm <string(1-128)> | key <string (1-64)> | keyid <value>}`

Parameter Description

- `realm<string(1-128)` - Configures the unique name of the container for the HMAC-MD5 (Hash Message Authentication Code - Message Digest 5) authentication key.This value is a string of size varying between 1 and 128.
- `key<string (1-64)>` - Configures the HMAC-MD5 key string which is used to authenticate the information-request message. This value is a string of size varying between 1 and 64.
- `keyid<value>` - Configures the Key identifier which is transmitted in information-request message as part of authentication information.The server searches in its local database, using this key identifier for the related key to calculate the HMAC. This value ranges between 0 and 4294967295.

Mode Interface Configuration mode(Vlan Interface Mode / Router)

Default keyid - 1

☞ The DHCPv6 client functionality should be enabled in the interface, before executing this command.

Example

```
Your Product(config-if)# ipv6 dhcp authentication
client realm 1
```

Related Command(s)

- `no switchport` – Configures the port as router port
- `ipv6 address dhcp` – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client
- `show ipv6 dhcp interface` – Displays the configuration information and also the DHCPv6 information received from the server for client, relay and server interfaces

35.1.6 ipv6 dhcp client-id type

Command Objective This command configures the DUID (DHCP Unique Identifier) type to be used for the client identifier. DUID consists of a two-octet type code represented in network byte order and a variable number of octets, to make an actual identifier. This DUID is used to identify the client in messages where the client sends a client identifier TLV (Type Length Value) in the information-request message. The Clients MUST treat DUIDs as opaque values and must compare DUIDs for equality Clients.

Syntax `ipv6 dhcp client-id type {llt | en | ll}`

Parameter Description

- `llt` - Configures the DUID which is formed based on LLT (Link-Layer Address plus Time). The DHCPv6 client uses the link layer address of the interface and current system time value for the client identifier option TLV value. This type of DUID consists of a two octet type field containing the value one, a two octet hardware type code, four octets containing a time value, and a link-layer address of any one network interface that is connected to the DHCP device at the time of generation of the DUID.
  - For client ID configured as llt, the DHCPv6 client and server should:
  - Compulsorily have a stable storage.
  - Store DUID-LLT in stable storage.
  - Continue to use DUID-LLT, even if network interface used to generate the DUID-LLT is removed.
  - Attempt to configure the time prior to generation of DUID, if possible, and should use time source (For example, real-time clock) for generating the DUID, even if the source is not configurable prior to the generation of the DUID.
- `en` - Configures the DUID which is assigned by the vendor based on EN (Enterprise Number). The DHCPv6 client uses the vendor-assigned unique ID based on the EN for the client identifier option TLV value. This type of DUID consists of vendor's registered private enterprise number as maintained by IANA (Internet Assigned Numbers Authority) and a unique identifier assigned by the vendor.
  - For client ID configured as en:
  - The identifier assigned by the vendor should be unique to device.
  - The unique identifier should be assigned to the device during its manufacture itself and should be stored in a non-volatile storage.
  - The generated DUID should be recorded in a non-erasable storage.
- `ll` - Configures the DUID which is formed based on LL (Link-layer Address). The DHCPv6 client uses the link layer address for the client identifier option TLV value. This type of DUID consists of two octets containing the DUID type 3, a two octet network hardware type code, and a link-layer address of any one network interface that is permanently connected to the client or server device.

- For client ID configured as ll:
- DHCP-LL should not be used by clients or servers that cannot tell whether or not a network interface is permanently attached to the device on which the DHCP client is running.
- Same DHCP-LL should be used in configuring all network interfaces connected to the device, regardless of usage of any interface's link-layer address to generate the DUID

Mode Interface Configuration mode(Vlan Interface Mode / Router)

Default `llt`

☞ The DHCPv6 client functionality should be enabled in the interface, before executing this command.

Example

```
Your Product(config-if)# ipv6 dhcp client-id type ll
```

Related Command(s)

- `no switchport` – Configures the port as router port
- `ipv6 address dhcp` – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client
- `show ipv6 dhcp interface` – Displays the configuration information and also the DHCPv6 information received from the server for client, relay and server interfaces

---

35.1.7 ipv6 dhcp client-id interface

Command Objective This command configures the interface that is used in the formation of the DUID based on LLT or on LL.

Syntax

```
ipv6 dhcp client-id interface {<interface-type>
<interface-id> }
```

Parameter Description

- `<interface-type>` - Configures DHCPv6 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.
  - internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Configures DHCPv6 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 or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

Mode Interface Configuration mode (Vlan Interface Mode / Router)

Default For a default, an arbitrary interface value is used.

☞ This command executes only if

- The DHCPv6 client functionality is enabled in the interface
- The physical interface that is configured to be used in the formation of DUID is configured as router port.

Example

```
Your Product(config-if)# ipv6 dhcp client-id
interface gigabitethernet 0/2
```

Related Command(s)

- `no switchport` – Configures the port as router port
- `ipv6 address dhcp` – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client
- `show ipv6 dhcp interface` - Displays DHCPv6 interface specific information.

35.1.8 ipv6 dhcp timer

Command Objective

This command is used to set the various timer parameters for a retransmission algorithm of the information-request message. The no form of the command is used to reset the timer parameters to the default value.

By default, the client calculates the retransmission time for the information-request message using the following formula:

RT = IRT + RAND * IRT

Where

RT - Retransmission Time

IRT - Initial Retransmission Time

RAND - Random number between -0.1 and +0.1

If the calculated RT becomes greater than the MRT (Maximum Retransmission Time), then the client calculates the RT using the following formula:

RT = MRT + RAND * MRT

Where

RT - Retransmission Time

MRT - Maximum Retransmission Time

RAND - Random number between -0.1 and +0.1

Syntax

```
ipv6 dhcp timer { irt <value(1-255)> | mrt <value(0-120)> | mrc <value(0-10)> | mrd <value(0-100)>}

no ipv6 dhcp timer [( irt | mrt | mrc | mrd }]
```

Parameter Description

- `irt<value(1-255)>` - Configures the initial retransmission time value. This value ranges between 1 and 255 seconds.
- `mrt<value(0-120)>` - Configures retransmission time value. This value ranges between 0 and 120 seconds.
- `mrc<value(0-10)>` - Configures the maximum retransmission count value. This value ranges between 0 and 10. If MRC (Maximum Retransmission Count) is zero, client continues to transmit the information-request message until it receives a reply response. If MRC is non-zero, client terminates the information-request message exchange and considers it as fail, on transmitting the information-request message MRC time.

- **mrd<value(0-100)>** - Configures the maximum retransmission delay value. This value ranges between 0 and 100 seconds. If MRD (Maximum Retransmission Delay) is zero, client continues to transmit the information-request message until it receives a reply response. If MRD is non-zero, client terminates the information-request message exchange and considers it as fail, once MRD is elapsed since the initial transmission of the message.

Mode Interface Configuration mode (Vlan Interface Mode / Router)

Default

- irt – 1
- mrt – 120
- mrc – 0
- mrd - 0

☞ DHCPv6 client functionality should be enabled in the interface, before executing this command.

Example

```
Your Product(config-if)# ipv6 dhcp timer irt 10
```

Related Command(s)

- **no switchport** – Configures the port as router port
- **ipv6 address dhcp** – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client
- **show ipv6 dhcp interface** – Displays the configuration information and also the DHCPv6 information received from the server for client, relay and server interfaces

---

35.1.9 ipv6 dhcp client information refresh minimum

Command Objective

This command sets the minimum refresh timer value for the information-request message, at the client side. The client once again sends information-request message to the server for acquiring configuration information, if the refresh timer is expired. The configured minimum refresh timer value is used, if an information refresh time option sent by the server is less than the configured value. This value ranges between 600 and 4294967295 seconds.

The no form of the command sets the refresh timer value to default value.

Syntax

```
ipv6 dhcp client information refresh minimum
<seconds value(600-4294967295)>

no ipv6 dhcp client information refresh minimum
```

Mode

Interface Configuration mode(Vlan Interface Mode / Router)

Default

86400 Seconds (24 Hours)

☞ The DHCPv6 client functionality should be enabled in the interface, before executing this command.

Example

```
Your Product(config-if)# ipv6 dhcp client
information refresh minimum 10000
```

Related Command(s)

- `no switchport` – Configures the port as router port
- `ipv6 address dhcp` – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client
- `show ipv6 dhcp interface` – Displays the configuration information and also the DHCPv6 information received from the server for client, relay and server interfaces

---

35.1.10 debug ipv6 dhcp client

Command Objective This command sets the debug traces for the DHCPv6 client.

The no form of the command resets the debug traces for the DHCPv6 client.

Syntax

```
debug ipv6 dhcp client {[init-shut] [mgmt] [ctrl] [pkt]
 [resource] [fail] [buffer] [critical] | [all]}

no debug ipv6 dhcp client {[init-shut] [mgmt] [ctrl] [pkt]
[resource] [fail] [buffer] [critical] | [all]}
```

Parameter Description

- `init-shut` – Generates debug messages for Init and shutdown traces.These traces are used during the module initialization and shutdown, and for cases such as failure of RBTree creation and so on.
- `mgmt` - Generates debug messages for Management traces.
- `ctrl` - Generates debug messages for Control plane traces. These traces are used for cases such as MBSM card removal, failure of state change and so on.
- `pkt` - Generates debug messages for Packet dump traces. These traces are used during the reception and transmission of packets.
- `resource` - Generates debug messages for Traces related to all resources such as memory, data structure and the like. These traces are used for failure of memory allocation and so on.
- `fail` - Generates debug messages for All failure traces. These traces are used for all valid and invalid failures. The valid failures represent the expected error. The invalid failures represent the unexpected error.
- `buffer` - Generates debug messages for buffer allocation / release traces.
- `critical` - Generates debug messages for SL (Stateless)-DHCPv6 client critical traces. These traces are used for cases such as failure of RBTree addition, failure to program the hardware, and so on.
- `all` - Generates debug messages for All traces.

Mode Privileged Exec Mode / User Exec Mode

Default critical

Example

```
Your Product# debug ipv6 dhcp client mgmt
```

35.1.11 clear ipv6 dhcp client statistics

Command Objective This command clears the DHCPv6 client statistics for the specified interface or all the interfaces.

Syntax

```
clear ipv6 dhcp client statistics [interface {vlan
<VlanId(1-4094)> | <interface-type> <interface-id>}]
```

Parameter Description

- `vlan<VlanId(1-4094)>` - Configures DHCPv6 for the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
- `<interface-type>` - Configures DHCPv6 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.
  - internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Configures DHCPv6for 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 or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

Mode Privileged Exec Mode

Example

```
Your Product# clear ipv6 dhcp client statistics
interface gigabitethernet 0/1
```

Related Command(s)

- `ipv6 address dhcp` – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client
- `show ipv6 dhcp client statistics` – Displays the DHCPv6 client statistics

35.1.12 show ipv6 dhcp

Command Objective This command displays the configuration information.

Syntax `show ipv6 dhcp`

Mode Privileged Exec Mode

Example

```
Your Product# show ipv6 dhcp
Client information:
  Listen UDP port      : 546
  Transmit UDP port : 547
  Sys log status : disabled
  SNMP traps      : none
Server information:
Listen UDP port             : 547
Client Transmit          UDP port      : 546
Relay Transmit UDP port  : 547
Sys log status              : disabled
SNMP traps                  : none
Authentication Information:
Client DUID : 636c69656e7431
Realm Name                : real1
Key Value                 : 1
Key Identifier : 74:72:69:61:6c
Relay information:
Listen UDP port             : 547
Client Transmit          UDP port      : 546
Server Transmit          UDP port      : 547
Sys log status              : disabled
SNMP traps                  : none
```

Related Command(s)

- `snmp-server enable traps ipv6 dhcp client` – Enables the SNMP traps for DHCPv6 client
- `ipv6 dhcp client port` – Configures the listen or transmit UDP ports
- `ipv6 dhcp client syslog` – Enables or disables the syslog generation

35.1.13 show ipv6 dhcp interface

Command Objective This command displays the configuration information and also the DHCPv6 information received from the server for client, relay and server interfaces.

Syntax

```
show ipv6 dhcp interface [ {vlan <VlanId(1-4094)>
| <interface-type> <interface-id>} | mgmt ]
```

Parameter Description

- `vlan<VlanId(1-4094)>` - Displays DHCPv6 for the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
- `<interface-type>` - Displays DHCPv6 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>` - Displays DHCPv6for 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 is provided, for interface types i-lan. For example: 1 represents i-lan ID.
- `mgmt` - Displays DHCPv6 for management interface.

Mode Privileged Exec Mode

Example

```
Your Product# show ipv6 dhcp interface
gigabitethernet 0/3 is in client mode

 DHCPv6 unique type(DUID Type) : Link-layer Address Plus
Time

  DHCPv6 unique identifier(DUID):
00010002000031b9fe8000000000000020102fffe0304
```

```
                                    01
  Minimum          Refresh      Time   :     86400 sec
  Current          Refresh      Time   :     86400 sec
Retransmission counters:
Maximum Ret Count : 0
Maximum Ret Delay   : 0     sec
Maximum Ret Time    : 120   sec
Initial Ret Time    : 1     sec
Current Ret Time    : 0     sec
Authentication information:
Realm Name    : -
Key Identifier : -
Key value     : 1
List of known servers:
Address    : fe80::202:2ff:fe03:401
DUID :
0001000200001b5bfe8000000000000020302fffe030401
Preference : 5
Status Code   : (Success)-SUCCESS
SIP domain list : Aricent.com
SIP servers   :fe80::200d:88ff:fe67:6666
DNS servers   : e80::200d:88ff:fe67:6666
DNS search list  : Aricent.com
```

Related Command(s)

- **ipv6 address dhcp** – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client
- **ipv6 dhcp authentication client** – Defines the domain, client identifier and the corresponding authentication MD5 (Message Digest 5) keys used to authenticate the information-request message and validate reply message
- **ipv6 dhcp client-id type** – Configures the DUID type to be used for the client identifier

- **ipv6 dhcp timer** – Configures various timer parameters for a retransmission algorithm of the information-request message
- **ipv6 dhcp client information refresh minimum** – Sets the minimum refresh timer value for the information-request message, at the client side

---

35.1.14 show ipv6 dhcp client statistics

Command Objective This command displays the DHCPv6 client statistics such as number of PDUs (Protocol Data Units) transmitted / received, for the specified interface or all the interfaces.

Syntax

```
show ipv6 dhcp client statistics [interface {vlan
<VlanId(1-4094)> | <interface-type> <interface-id>}]
```

Parameter Description

- `vlan<VlanId(1-4094)>` - Displays DHCPv6 for the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
- `<interface-type>` - Displays DHCPv6 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.
  - internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Displays DHCPv6for 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 internal-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

Mode Privileged Exec Mode

Example

```
Your Product# show ipv6 dhcp client statistics
gigabitethernet 0/1
  Transmitted:
   information-request : 1
```

```
  Received:
invalid    : 0
hmac-failure     : 0
vlan 1
Transmitted:
information-request : 1
Received:
reply: 1
invalid    : 0
hmac-failure     : 0
```

Your Product# show ipv6 dhcp client statistics interface gigabitethernet 0/1

```
gigabitethernet 0/1
Transmitted:
information-request : 1
Received:
reply: 1
invalid    : 0
hmac-failure     : 0
```

Your Product# show ipv6 dhcp client statistics interface vlan 1

```
vlan 1
Transmitted:
information-request : 1
Received:
reply: 1
invalid    : 0
hmac-failure     : 0
```

Related Command(s)

- **ipv6 address dhcp** – Enables the DHCPv6 client functionality over the interface and requests for configuration information from the client

- `clear ipv6 dhcp client statistics` – Clears the DHCPv6 client statistics for the specified interface or all the interfaces

---

35.2 DHCPv6 Relay

The DHCPv6 relay is an intermediate node that relays DHCP messages between the DHCPv6 clients and DHCPv6 servers on different links.

The list of CLI commands for the configuration of DHCPv6 Relay is as follows

- snmp-server enable traps ipv6 dhcp relay
- ipv6 dhcp relay syslog
- ipv6 dhcp relay port
- ipv6 dhcp relay
- ipv6 dhcp relay hop-threshold
- debug ipv6 dhcp relay
- clear ipv6 dhcp relay statistics
- show ipv6 dhcpshow ipv6 dhcp interface
- show ipv6 dhcp relay statistics
- ipv6 dhcp relay remote-id
- ipv6 dhcp relay remote-id type
- ipv6 dhcp relay remote-id duid
- ipv6 dhcp relay remote-id userDefined

35.2.1 snmp-server enable traps ipv6 dhcp relay

Command Objective

This command enables the transmission of SNMP traps notification messages for DHCPv6 relay. It enables all the traps, when executed without any option.

This command allows to enable multiple SNMP traps for the DHCPv6 relay. That is, both the specified trap notifications can be enabled one after the other.

The no form of the command disables the SNMP traps for the DHCPv6 relay. It sets the trap as none, when executed without any option.

Syntax

```
snmp-server enable traps ipv6 dhcp relay [invalid-pkt] [max-hop-count]

no snmp-server enable traps ipv6 dhcp relay [invalid-pkt] [max-hop-count]
```

Parameter Description

- `invalid-pkt` - Enables or disables the transmission of invalid packet trap notification, based on the Relay agent which declares the received notification message as invalid. This trap notification is generated, when the received message is invalid or when the AdminControl value is set with value 0.
- `max-hop-count` - Enables or disables the transmission of maximum hop count trap notification, based on the relay agent which receives the relay forward message with hop count value is less then one configured hop count. This trap notification is generated, when the relay agent is not able to add the relay header, as the received hop count value is equal to the configured maximum hop threshold limit.

Mode

Global Configuration mode

Default

SNMP traps are disabled for the DHCPv6 relay.

Example

```
Your Product(config)# snmp-server enable traps ipv6 dhcp relay max-hop-count
```

Related Command(s)

- `show ipv6 dhcp` – Displays the DHCPv6 relay global configurations

35.2.2 ipv6 dhcp relay syslog

Command Objective This command enables or disables the transmission of syslog notification messages for the DHCPv6 relay

---

Syntax **ipv6 dhcp relay syslog {enable | disable}**

Parameter Description

- **enable** - Configures the DHCPv6 relay to generate syslog messages when the transmission of syslog notification messages enabled.
- **disable** - Configures the DHCPv6 relay not to generate any syslog messages, when the transmission of syslog notification messages is disabled

---

Mode Global Configuration mode

Default Disable

Example **Your Product(config)# ipv6 dhcp relay syslog enable**

Related Command(s)

- **show ipv6 dhcp** – Displays the DHCPv6 relay global configurations

---

35.2.3 ipv6 dhcp relay port

Command Objective This command sets the listen UDP port number, and client and server transmit and to configure the port on which the DHCPv6 relay agent will listen on. This command facilitates the DHCPv6 relay to co-exist with the DHCPv6 server which can listen on a different port.

Syntax

```
ipv6 dhcp relay port {listen <value(1-65535)> | client transmit <value(1-65535)> | server transmit <value(1-65535)>}
```

Parameter Description

- `listen<value(1-65535)>` - Configures the UDP port number on which the DHCPv6 relay should listen.This value ranges between 1 and 65535.
- `client transmit<value(1-65535)>` - Configures the UDP port number on which the DHCPv6 relay sends reply message. This value ranges between 1 and 65535.
- `server transmit<value(1-65535)>` - Configures the UDP port number on which the DHCPv6 relay sends relay-forward message. This value ranges between 1 and 65535.

Mode Global Configuration mode

Default

- listen – 547
- client transmit - 546
- server transmit – 547

Example

```
Your Product(config)# ipv6 dhcp relay port listen 34
```

Related Command(s)

- `show ipv6 dhcp` – Displays the DHCPv6 relay global configurations

35.2.4 ipv6 dhcp relay

Command Objective

This command enables the relay feature on an interface and optionally sets the destination server address and configures an outgoing interface.

The no form of the command disables the relay feature on the interface and optionally unsets the destination server address and the outgoing interface

---

Syntax

```
ipv6 dhcp relay [destination <prefix> {link-local |
<prefix Len> } [interface {Vlan <vlan-id (1-4094)> |
<interface-type> <interface-id>}]]

no ipv6 dhcp relay [destination <prefix> {link-local
| <prefix Len> } [interface {Vlan <vlan-id (1-4094)>
| <interface-type> <interface-id>}]]
```

Parameter Description

- `destination <prefix>` - Configures the IPv6 address of the destination DHCP server.
- `link-local` - Configures the Link-local type IPv6 address of the DHCP Relay.
- `<prefix Len>` - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value ranges between 0 to 128.
- `Vlan<vlan-id (1-4094)>` - Configures DHCPv6 for the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
- `<interface-type>` - Configures DHCPv6 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>` - Configures DHCPv6 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 is provided for interface types. For example: 1 represents i-lan ID.

Mode Interface Configuration mode (Vlan Interface Mode / Router)

Default DHCPv6 relay feature is disabled.

Example

```
Your Product(config-if)# ipv6 dhcp relay destination
1111::2222 128 interface vlan 1
```

Related Command(s)

- `no switchport` – Configures the port as router port
- `ipv6 dhcp relay hop-threshold` – Sets the hop threshold limit for the DHCPv6 relay packets
- `ipv6 dhcp relay remote-id type` - Sets the type of the remote-id option for the DHCPv6 relay
- `ipv6 dhcp relay remote-id duid` - Configures DHCPv6 Relay Unique Identifier (DUID) value for the interface
- `clear ipv6 dhcp relay statistics` – Clears DHCPv6 relay transmit and receive statistics for a particular interface or for all the interfaces
- `ipv6 dhcp relay remote-id userDefined` - Configures DHCPv6 Relay userdefined value for the interface
- `show ipv6 dhcp interfcae` – Displays the DHCPv6 relay configurations on a particular interface or all the interfaces
- `show ipv6 dhcp relay statistics` – Displays the DHCPv6 relay statistics on a particular interface or on all the interface

---

35.2.5 ipv6 dhcp relay hop-threshold

Command Objective

This command sets the hop threshold limit for the DHCPv6 relay packets. The limit represents the maximum number of hop count allowed by relay agent to pass through it. Packets are dropped at the relay agent, if the hop count in DHCP message is greater than the threshold limit. This value ranges between 0 and 32.

The no form of the command resets the threshold limit to default value.

Syntax

```
ipv6 dhcp relay hop-threshold <count>

no ipv6 dhcp relay hop-threshold
```

Mode

Interface Configuration mode (Vlan Interface Mode / Router)

Default

4

☞ The DHCPv6 relay feature should be enabled in the interface, before executing this command.

Example

```
Your Product(config-if)# ipv6 dhcp relay hop-threshold 3
```

Related Command(s)

- `no switchport` – Configures the port as router port
- `ipv6 dhcp relay`- Enables the relay feature on an interface and optionally sets the destination server address and configures an outgoing interface
- `show ipv6 dhcp interface` – Displays the DHCPv6 relay configurations on a particular interface or all the interfaces

---

35.2.6 debug ipv6 dhcp relay

Command Objective This command sets the debug traces for the DHCPv6 relay.

The no form of the command resets the debug traces for the DHCPv6 relay.

Syntax

```
debug ipv6 dhcp relay {[init-shut] [mgmt] [ctrl] [pkt]
[resource] [fail] [buffer] [critical] [all]}

no debug ipv6 dhcp relay {[init-shut] [mgmt] [ctrl]
[pkt] [resource] [fail] [buffer] [critical] [all]}
```

Parameter Description

- `init-shut` - Generates debug messages for Init and shutdown traces. These traces are used during the module initialization and shutdown, and for cases such as failure of RBTree creation and so on.
- `mgmt` - Generates debug messages for Management traces.
- `ctrl` - Generates debug messages for Control plane traces. These traces are used for cases such as MBSM card removal, failure of state change and so on.
- `pkt` - Generates debug messages for Packet dump traces. These traces are used during the reception and transmission of packets.
- `resource` - Generates debug messages for Traces related to all resources such as memory, data structure and the like. These traces are used for failure of memory allocation and so on.
- `fail` - Generates debug messages for all failure traces. These traces are used for all valid and invalid failures. The valid failures represent the expected error. The invalid failures represent the unexpected error.
- `buffer` - Generates debug messages for Buffer allocation / release traces.
- `critical` - Generates debug messages for SL-DHCPv6 relay critical traces. These traces are used for cases such as failure of RBTree addition, failure to program the hardware, and so on.
- `all` - Generates debug messages for All traces.

Mode Privileged Exec Mode / User Exec Mode

Default Critical

Example

```
Your Product# debug ipv6 dhcp relay all
```

35.2.7 clear ipv6 dhcp relay statistics

Command Objective This command clears DHCPv6 relay transmit and receive statistics for a particular interface or for all the interfaces.

Syntax

```
clear ipv6 dhcp relay statistics [interface {vlan
<VlanId(1-4094)> |<interface-type> <interface-id>}]
```

Parameter Description

- `vlan<VlanId(1-4094)>` - Configures DHCPv6 for the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
- `<interface-type>` - Configures DHCPv6 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.
  - internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Configures DHCPv6 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 or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

Mode Privileged Exec Mode

Example

```
Your Product# clear ipv6 dhcp relay statistics
```

Related Command(s)

- `ipv6 dhcp relay`– Enables the relay feature on an interface and optionally sets the destination server address and configures an outgoing interface

- **show ipv6 dhcp relay statistics** – Displays the DHCPv6 relay statistics on a particular interface or on all the interface

---

35.2.8 show ipv6 dhcp

Command Objective This command displays the DHCPv6 relay global configurations.

Syntax `show ipv6 dhcp`

Mode Privileged Exec Mode

Example

```
Your Product# show ipv6 dhcp
Client information:
  Listen UDP port      : 546
  Transmit UDP port: 547
  Sys log status : disabled
  SNMP traps     : none
Server information:
Listen UDP port          : 547
Client Transmit UDP port : 546
Relay Transmit UDP port  : 547
Sys log status           : disabled
SNMP traps               : none
Authentication Information:
Client DUID : 636c69656e7431
Realm Name               : real1
Key Value                : 1
Key Identifier : 74:72:69:61:6c
Relay information:
Listen UDP port          : 547
Client Transmit UDP port : 546
Server Transmit UDP port : 547
Sys log status           : disabled
SNMP traps               : none
Remote-ID(Option 37)     : enabled
```

Related Command(s)

- `snmp-server enable traps ipv6 dhcp` – Enables the SNMP traps for DHCPv6 relay
- `ipv6 dhcp relay syslog` – Enables or disables the syslog feature for the DHCPv6 relay
- `ipv6 dhcp relay port` – Sets the listen UDP port number, and client and server transmit UDP port numbers
- `ipv6 dhcp relay remote-id` - Enables / disables insertion of DHCPv6 option37-Remote-id option in DHCPv6 Relay FWD messages

---

35.2.9 show ipv6 dhcp interface

Command Objective This command displays the DHCPv6 relay configurations on a particular interface or all the interfaces.

Syntax

```
show ipv6 dhcp interface [ {vlan <VlanId(1-4094)> |
<interface-type> <interface-id>}]
```

Parameter Description

- `vlan<VlanId(1-4094)>` - Displays DHCPv6 for the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
- `<interface-type>` - Displays DHCPv6 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>` - Displays DHCPv6 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.

Mode Privileged Exec Mode

Example

```
Your Product# show ipv6 dhcp interface
gigabitethernet 0/4 is in relay mode
  HopThreshold value : 4
  Remote-Id       Option Type   : duid
  Remote-IdOption Value : 12:12:34:90
  Server Address  : unicast to configured servers only
```

```
fe80::219:dbff:fe88:dc07 :      Gi0/3
```

Related Command(s)

- **ipv6 dhcp relay** – Enables the relay feature on an interface and optionally sets the destination server address and configures an outgoing interface
- **ipv6 dhcp relay hop-threshold** – Sets the hop threshold limit for the DHCPv6 relay packets
- **ipv6 dhcp relay remote-id type** - Sets the type of the remote-id option for the DHCPv6 relay
- **ipv6 dhcp relay remote-id userDefined** - Configures DHCPv6 Relay userdefined value for the interface
- **ipv6 dhcp relay remote-id duid** - Configures DHCPv6 Relay Unique Identifier (DUID) value for the interface

---

35.2.10 show ipv6 dhcp relay statistics

Command Objective This command displays the DHCPv6 relay statistics on a particular interface or on all the interfaces.

Syntax

```
show ipv6 dhcp relay statistics [interface {vlan
<VlanId(1-4094)> | <interface-type> <interface-id>} ]
```

Parameter Description

- `vlan<VlanId(1-4094)>` - Displays DHCPv6 for the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
- `<interface-type>` - Displays DHCPv6 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.
  - **internal-lan** – Internal LAN created on a bridge per IEEE 802.1ap.
  - **port-channel** – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Displays DHCPv6 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 internal-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only internal-lan or port-channel ID is provided, for interface types i-lan and port-channel. For example: 1 represents internal-lan and port-channel ID.

Mode Privileged Exec Mode

Example

```
Your Product# show ipv6    dhcp relay statistics
     gigabitethernet 0/4
     Received:
```

```
information-request    : 1
relay-forward     : 0
relay-reply : 1
invalid     : 0
```

Related Command(s)

- **ipv6 dhcp relay** – Enables the relay feature on an interface and optionally sets the destination server address and configures an outgoing interface
- **clear ipv6 dhcp relay statistics** – Clears DHCPv6 relay transmit and receive statistics for a particular interface or for all the interface

---

35.2.11 ipv6 dhcp relay remote-id

Command Objective This command enables / disables insertion of DHCPv6 option37-Remote-id

---

Syntax `ipv6 dhcp relay remote-id {enable | disable}`

Parameter Description

- `enable` - Enables insertion of DHCPv6 option 37 Remote –Id in DHCPv6 Relay Forward Messages
- `disable` - Disables insertion of DHCPv6 option 37 Remote –Id in DHCPv6 Relay Forward Messages

---

Mode Global Configuration Mode

Default Remote-Id Option is disabled.

Example

```
Your Product(config)# ipv6 dhcp relay remote-id enable
```

Related Command(s)

- `ipv6 dhcp relay remote-id type` - Sets the type of the remote-id option for the DHCPv6 relay.
- `ipv6 dhcp relay remote-id duid` - Configures DHCPv6 Relay Unique Identifier (DUID) value for the interface.
- `ipv6 dhcp relay remote-id userDefined` - Configures DHCPv6 Relay userdefined value for the interface
- `show ipv6 dhcp` – Displays the DHCPv6 relay global configurations.

35.2.12 ipv6 dhcp relay remote-id type

Command Objective This command sets the type of the remote-id option for the DHCPv6 relay.

Syntax

```
ipv6 dhcp relay remote-id type {duid | switch-name |
mgmt-ip | userDefined }
```

Parameter Description

- `duid` - Configures the remote-id option as DHCP Unique Identifier.
- `switch-name` - Configures the remote-id option as Current System Name.
- `mgmt-ip` - Configures the remote-id option as Management IP of the system.
- `userDefined` - Sets the type of the remote-id option for the DHCPv6 relay as userDefined

---

Mode Interface Configuration mode(Vlan Interface Mode / Router)

Default switch-name

Example

```
Your Product(config-if)# ipv6 dhcp relay remote-id
type duid
```

☞ This command executes only if

- The DHCPv6 relay feature is enabled in the interface
- Remote-Id option is enabled

Related Command(s)

- `no switchport` – Configures the port as router port.
- `ipv6 dhcp relay`– Enables the relay feature on an interface and optionally sets the destination server address and configures an outgoing interface.
- `ipv6 dhcp relay remote-id` - Enables / disables insertion of DHCPv6 option37-Remote-id option in DHCPv6 Relay FWD messages.
- `show ipv6 dhcp interface` – Displays the DHCPv6 relay configurations on a particular interface or all the interfaces.

35.2.13 ipv6 dhcp relay remote-id duid

Command Objective

This command configures DHCPv6 Relay Unique Identifier (DUID) value for the interface. DHCPv6 servers use the DUID to make decisions about information such as addresses, delegated prefixes, configuration parameters etc. that the client is to receive.

Relay Agent uses the DUID to have a unique remote-id for its enterprise number, as sequence of enterprise number followed by remote-id must be globally unique.

DHCPv6 Relay DUID is a 128 octets long identifier, which can have Link-Layer Address as DUID octets or can have Link-Layer address along with some other parameter having variable octets or can have any sequence of octets representing unique DUID.

Syntax

```
ipv6 dhcp relay remote-id duid <duid-id string(128)>
```

Mode

Interface Configuration mode (Vlan Interface Mode / Router)

Default

All octets are zero

Example

```
Your Product(config-if)# ipv6 dhcp relay remote-id
duid 12:12:aa
```

This command executes only if

- The DHCPv6 relay feature is enabled in the interface
- Remote-Id option is enabled

Related Command(s)

- `no switchport` – Configures the port as router port.
- `ipv6 dhcp relay`- Enables the relay feature on an interface and optionally sets the destination server address and configures an outgoing interface.
- `ipv6 dhcp relay remote-id` - Enables / disables insertion of DHCPv6 option37-Remote-id option in DHCPv6 Relay FWD messages.
- `show ipv6 dhcp interface` – Displays the DHCPv6 relay configurations on a particular interface or all the interfaces.

35.2.14 ipv6 dhcp relay remote-id userDefined

Command Objective This command configures DHCPv6 Relay userdefined value for this interface.

Syntax `ipv6 dhcp relay remote-id userDefined <user-specific-ascii string(128)>`

Mode Interface Configuration mode(Vlan Interface Mode / Router)

Example

```
Your Product(config-if)# ipv6 dhcp relay remote-id userDefined 1
```

☞ This command executes only if

- The DHCPv6 relay feature is enabled in the interface
- Remote-Id option is enabled

Related Command(s)

- `no switchport` – Configures the port as router port.
- `ipv6 dhcp relay`- Enables the relay feature on an interface and optionally sets the destination server address and configures an outgoing interface.
- `ipv6 dhcp relay remote-id` - Enables / disables insertion of DHCPv6 option37-Remote-id option in DHCPv6 Relay FWD messages.
- `show ipv6 dhcp interface` – Displays the DHCPv6 relay configurations on a particular interface or all the interfaces.

35.3 DHCPv6 Server

The DHCPv6 server is a node that responds to requests from the DHCPv6 clients. It can be on the same link as the clients or on the different link. It receives DHCP messages from the clients using a reserved, link-scoped multicast address.

The list of CLI commands for the configuration of DHCPv6 Server is as follows:

- snmp-server enable traps ipv6 dhcp server
- ipv6 dhcp server port
- ipv6 dhcp server syslog
- ipv6 dhcp authentication server client-id
- ipv6 dhcp authentication
- ipv6 dhcp pool
- vendor-specific
- sub option
- link-address
- domain-name
- dns-server
- sip address
- sip domain-name
- option
- ipv6 dhcp server-id type
- ipv6 dhcp server-id interface
- information refresh
- ipv6 dhcp server
- debug ipv6 dhcp server
- clear ipv6 dhcp server statistics
- show ipv6 dhcp
- show ipv6 dhcp pool
- show ipv6 dhcp interface
- show ipv6 dhcp server statistics

35.3.1 snmp-server enable traps ipv6 dhcp server

Command Objective

This command enables the transmission of SNMP traps notification messages for DHCPv6 server. It enables all the traps, when executed without any option.

This command allows to enable multiple SNMP traps for the DHCPv6 client. That is, all the three specified trap notifications can be enabled one after the other.

The no form of the command disables the SNMP traps for the DHCPv6 server. It sets the trap as none, when executed without any option.

Syntax

```
snmp-server enable traps ipv6 dhcp server [unknown-tlv]
 [invalid-pkt] [auth-fail]

no snmp-server enable traps ipv6 dhcp server [unknown-tlv]
| [invalid-pkt] | [auth-fail]
```

Parameter Description

- `unknown-tlv` - Enables or disables the transmission of unknown TLV trap notification, based on the server which declares the received notification message as unknown TLV. This trap notification is generated, when received information-request or relay forward message contains invalid TLV type.
- `invalid-pkt` - Enables or disables the transmission of invalid packet trap notification, based on the server which declares the received notification message as invalid. This trap notification is generated, when the received information-request or relay forward message is invalid.
- `auth-fail` - Enables or disables the transmission of HMAC authentication fail trap notification, based on the server which declares the received notification message as authentication fail. This trap notification is generated, when the received information-request or relay forward message contains the authentication TLV and digest calculated at the server side that does not match with the received digest value. The digest is calculated at the server side with the realm and key ID values.

Mode

Global Configuration mode

Default

SNMP traps are disabled for the DHCPv6 server

Example

```
Your Product(config)# snmp-server enable traps ipv6
dhcp server auth-fail
```

Related Command(s)

- `show ipv6 dhcp` – Displays the various configuration information at server end

35.3.2 ipv6 dhcp server port

Command Objective This command configures the information-request listen, reply transmit and relay-reply transmit UDP ports. The Server process the received information request message and relay-forward only when destination port number in UDP Header is equal to configured listen port number.

Syntax `ipv6 dhcp server port {listen <value(1-65535)> | client transmit <value(1-65535)> | relay transmit <value(1-65535)>}`

Parameter Description

- `listen<value(1-65535)>` - Configures the UDP listen port number. This value ranges between 1 and 65535.
- `client transmit<value(1-65535)>` - Configures the UDP transmit port, which is set as the destination port number in UDP header of the reply message. This value ranges between 1 and 65535.
- `relay transmit<value(1-65535)>` - Configures the UDP transmit port, which is set as the destination port number in UDP header of the relay-reply message. This value ranges between 1 and 65535.

Mode Global Configuration mode

Default

- listen - 547
- client transmit - 546
- relay transmit – 547

Example

```
Your Product(config)# ipv6 dhcp server port listen 800
```

Related Command(s)

- `show ipv6 dhcp` – Displays the various configuration information at server end

---

35.3.3 ipv6 dhcp server syslog

Command Objective This command enables or disables the transmission of syslog notification messages for the DHCPv6 Server

---

Syntax `ipv6 dhcp server syslog {enable | disable}`

Parameter Description

- `enable` - Configures the DHCPv6 relay to generate syslog messages when the transmission of syslog notification messages enabled.
- `disable` - Configures the DHCPv6 relay not to generate any syslog messages, when the transmission of syslog notification messages is disabled

---

Mode Global Configuration mode

Default disable

Example

```
Your Product(config)# ipv6 dhcp server syslog enable
```

Related Command(s)

- `show ipv6 dhcp` – Displays the various configuration information at server end

---

35.3.4 ipv6 dhcp authentication server client-id

Command Objective

This command creates client configuration pool at the server and enters into the client information configuration mode. It allows to create multiple client configuration pools at the server.

The no form of the command deletes the client configuration pool maintained at the server.

Syntax

```
ipv6 dhcp authentication server client-id
<string(128)> {llt | en | ll}

no ipv6 dhcp authentication server client-id
string(1-128
```

Parameter Description

- `<string(128)>` - Configures the string as the name of the client. This value is a string of size varying between 1 and 128.
- `llt` - Generates DUID based on LLT (Link-Layer Address plus Time) and indicates that the DHCPv6 client uses the link layer address of the interface and current system time value for the client identifier option TLV value. This type of DUID consists of a two octet type field containing the value 1, a two octet hardware type code, four octets containing a time value, and a link-layer address of any one network interface that is connected to the DHCP device at the time of generation of the DUID.
  - For client ID configured as llt, the DHCPv6 client and server should:
    - Compulsorily have a stable storage.
    - Store DUID-LLT in stable storage.
    - Continue to use DUID-LLT, even if network interface used to generate the DUID-LLT is removed.
    - Attempt to configure the time prior to generation of DUID, if possible, and should use time source (For example, real-time clock) for generating the DUID, even if the source is not configurable prior to the generation of the DUID.
- `en` - Assigns DUID by the vendor based on EN and indicates that the DHCPv6 client uses the vendor-assigned unique ID based on the EN for the client identifier option TLV value. This type of DUID consists of vendor's registered private enterprise number as maintained by IANA and a unique identifier assigned by the vendor.
  - For client ID configured as en:
    - The identifier assigned by the vendor should be unique to device.
    - The unique identifier should be assigned to the device during its manufacture itself and should be stored in a non-volatile storage.
    - The generated DUID should be recorded in a non-erasable storage.
- `ll` - Generates DUID based on LL (Link-layer Address) and indicates that the DHCPv6 client uses the link layer address for the client identifier option TLV

value. This type of DUID consists of two octets containing the DUID type 3, a two octet network hardware type code, and a link-layer address of any one network interface that is permanently connected to the client or server device.

- For client ID configured as ll:
  - DHCP-LL should not be used by clients or servers that cannot tell whether or not a network interface is permanently attached to the device on which the DHCP client is running.
  - Same DHCP-LL should be used in configuring all network interfaces connected to the device, regardless of usage of any interface's link-layer address to generate the DUID.

Mode Global Configuration mode

Example

```
Your Product(config)# ipv6 dhcp authentication server
client-id client1 en

Your Product(config-d6clnt)#
```

Related Command(s)

- `ipv6 dhcp authentication` – Configures the realm and key value
- `show ipv6 dhcp` – Displays the various configuration information at server end

---

35.3.5 ipv6 dhcp authentication

Command Objective

This command configures the realm and key value through which the server authenticate the received information request with the HMAC MD5 algorithm when the received message contains the authentication option tlv.

The no form of the command deletes the realm and key value.

Syntax

```
ipv6 dhcp authentication realm <string (1-128)> key
<string(1-64)>

no ipv6 dhcp authentication realm <string (1-128)>
[key <string(1-64)>
```

Parameter Description

- `realm<string (1-128)>` - Configures the name of the container used to store the HMAC-MD5 authentication keys, where realms are container for authentication information.The maximum string size is 128.
- `key<string(1-64)>` - Configures the HMAC-MD5 key string used to authenticate the information-request message, where the authentication key Ids are assigned to the clients. The maximum string size is 64.

Mode

Client Information Configuration mode

- The client configuration pool should be created, before configuring the realm and key value.
- When this command is executed for next client ID with the same container name, the key-identifier and key value of the previous client-ID is inherited to the new client ID and then the concerned key identifier and key value are assigned to the new client ID based on the configuration.

Example

```
Your Product(config-d6clnt)# ipv6 dhcp
authentication realm products key ISS
```

Related Command(s)

- `ipv6 dhcp authentication server client-id` – Creates client configuration pool at the server and enters into the client pool configuration mode
- `show ipv6 dhcp` – Displays the various configuration information at server end

---

35.3.6 ipv6 dhcp pool

Command Objective

This command creates a DHCP6 server pool and enters into IPv6 DHCP pool configuration mode where the pool is configured independently of the DHCPv6 service. The configuration information pool is a named entity that includes information about available configuration parameters and policies that control assignment of the parameters to clients from the pool. The maximum string size is 64.

The no form of the command deletes the DHCP6 server pool. Need to remove the configured option manually before deleting a pool.

Syntax

```
ipv6 dhcp pool <string (1-64)>
no ipv6 dhcp pool <string (1-64)>
```

Mode

Global Configuration mode

Example

```
Your Product(config)# ipv6 dhcp pool dhcp6pool1
Your Product(config-d6pool)#
```

Related Command(s)

- `vendor-specific` – Enters into vendor-specific configuration mode with vendor-specific identification number
- `sub option` – Enables a sub-option of the configured vendor specific information
- `link-address` – Sets a link-address IPv6 prefix
- `domain-name` – Defines the DNS domain suffix which is provided to the client in reply message on request
- `dns-server` – Defines the DNS server IP address which is provided to the client in reply message on request
- `sip address` – Defines the SIP server IP address which is provided to the client in reply message on request
- `sip domain-name` – Defines the SIP domain name which is provided to the client in reply message on request
- `option` – Sets pool specific DHCP6 server option
- `ipv6 dhcp server-id type` – Configures the DUID type to be used for the server identifier
- `ipv6 dhcp server-id interface` – Configure the interface that is used in the formation of the DUID based on LLT or on LL
- `information refresh` – Configures the refresh time value that is to be sent to the client

- **show ipv6 dhcp pool** – Displays the DHCPv6 server pool information
- **show ipv6 dhcp interface** – Displays the various configuration information at server end for specified interface or all the interfaces

---

35.3.7 vendor-specific

Command Objective

This command enters into vendor-specific configuration mode with vendor-specific identification number and options which the server will reply in response to an information-request or relay-forward message. This value ranges between 1 and 2147483647.

The no form of the command deletes all configured vendor specific information.

Syntax

```
vendor-specific <vendor-id (1-2147483647)>

no vendor-specific <vendor-id (1-2147483647)>
```

Mode

IPv6 DHCP Pool Configuration mode

☞ The DHCPv6 server address pool should be created, before configuring the vendor specific information.

Example

```
Your Product(config-d6pool)# vendor-specific 10

Your Product(d6pool-vendor)#
```

Related Command(s)

- `ipv6 dhcp pool` – Creates a DHCP6 server address pool
- `sub option` – Enables a sub-option of the configured vendor specific information
- `show ipv6 dhcp pool` – Displays the DHCPv6 server pool information

35.3.8 sub option

Command Objective

This command enables a sub-option of the configured vendor specific information. This entry is not lost upon reboot; it is backed up by stable storage. Each entry in this table contains the required attribute values.

The no form of the command deletes the sub-option.

Syntax

```
sub option <option-id (1-4294967295)> { address
<IPv6-address> | ascii <ASCII-string> | hex
<hex_string>}

no sub option <option-id> { address <IPv6-address> |
ascii <ASCII-string> | hex <hex_string>}
```

Parameter Description

- `<option-id(1-4294967295)>` - Indicates a unique sub-option type. This value ranges between 1 and 4294967295.
- `address<IPv6-address>` - Configures an IPv6 address that can be provided as a sub-option value.
- `ascii<ASCII-string>` - Configures an ASCII string that can be provided as a sub-option value. The maximum string size is 255.
- `hex<hex_string>` - Configures a hexadecimal string that can be provided as a sub-option value. This value is an octet string of size varying between 1 and 32.

Mode

Vendor Specific Information Configuration mode

☞ The DHCPv6 server address pool should be created and the vendor-specific information should be configured, before enabling sub-option of the vendor specific information.

Example

```
Your Product(d6pool-vendor)# sub option 3 address
0000::1111
```

Related Command(s)

- `ipv6 dhcp pool` – Creates a DHCP6 server address pool
- `vendor-specific` – Enters into vendor-specific configuration mode with vendor-specific identification number
- `show ipv6 dhcp pool` - Displays the DHCPv6 server pool information.

35.3.9 link-address

Command Objective

This command sets a link-address IPv6 prefix. The server uses the configuration information pool, when an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix.

The no form of the command removes the link-address IPv6 prefix.

Syntax

```
link-address <IPV6-Prefix>
no link-address <IPV6-Prefix>
```

Mode

IPv6 DHCP Pool Configuration mode

☞ The DHCPv6 server address pool should be created, before executing this command.

Example

```
Your Product(config-d6pool)# link-address 2222::1111
```

Related Command(s)

- `ipv6 dhcp pool`– Creates a DHCP6 server address pool
- `show ipv6 dhcp pool`– Displays the DHCPv6 server pool information

35.3.10 domain-name

Command Objective

This command defines the DNS domain suffix which is provided to the client in reply message on request.

The no form of the command deletes the DNS domain suffix.

Syntax

```
domain-name <domain name> [preference <value (0-255)> ]
no domain-name <domain name>
```

Parameter Description

- `<domain name>` - Configures the domain name prefix that is used to resolve a domain name. the maximum string size is 64.
- `preference<value (0-255)>` - Configures the preference value of the pool. This value ranges between 0 and 255. The DHCPv6 client uses this value to select the best information on receiving multiple reply messages from different servers.

Mode

IPv6 DHCP Pool Configuration mode

Default

preference - 0

☞ The DHCPv6 server address pool should be created, before executing this command.

Example

```
Your Product(config-d6pool)# domain-name 34 preference 56
```

Related Command(s)

- `ipv6 dhcp pool`– Creates a DHCP6 server address pool
- `show ipv6 dhcp pool` – Displays the DHCPv6 server pool information

35.3.11 dns-server

Command Objective

This command defines the DNS server IP address which is provided to the client in reply message on request.

The no form of the command deletes the DNS server IP address.

Syntax

```
dns-server <ipv6-address>
no dns-server <ipv6-address>
```

Mode

IPv6 DHCP Pool Configuration mode

☞ The DHCPv6 server address pool should be created, before executing this command.

Example

```
Your Product(config-d6pool)# dns-server 3333::2222
```

Related Command(s)

- `ipv6 dhcp pool`– Creates a DHCP6 server address pool
- `show ipv6 dhcp pool` – Displays the DHCPv6 server pool information

35.3.12 sip address

Command Objective

This command defines the SIP server IP address which is provided to the client in reply message on request.

The no form of the command deletes the SIP server IP address.

Syntax

```
sip address <ipv6-address> [preference <value (0-255)> ]

no sip address <ipv6-address>
```

Parameter Description

- `<ipv6-address>` - Configures an IPv6 address that can be set as a SIP server.
- `preference<value (0-255)>` - Configures the preference value of the pool. This value ranges between 0 and 255. The DHCPv6 client uses this value to select the best information on receiving multiple reply messages from different servers.

Mode

IPv6 DHCP Pool Configuration mode

☞ The DHCPv6 server address pool should be created, before executing this command.

Example

```
Your Product(config-d6pool)# sip address 0000::2222
preference 34
```

Related Command(s)

- `ipv6 dhcp pool`– Creates a DHCP6 server address pool
- `show ipv6 dhcp pool` – Displays the DHCPv6 server pool information

35.3.13 sip domain-name

Command Objective

This command defines the SIP domain name which is provided to the client in reply message on request. The maximum string size is 64.

The no form of the command deletes the SIP domain name.

Syntax

```
sip domain-name <domain-name>

no sip domain-name <domain-name>
```

Mode

IPv6 DHCP Pool Configuration mode

☞ The DHCPv6 server address pool should be created, before executing this command.

Example

```
Your Product(config-d6pool)# sip domain-name sip
```

Related Command(s)

- `ipv6 dhcp pool`– Creates a DHCP6 server address pool
- `show ipv6 dhcp pool` – Displays the DHCPv6 server pool information

35.3.14 option

Command Objective

This command sets pool specific DHCP6 server option.

The no form of the command deletes the pool specific DHCP6 server option.

Syntax

```
option <code (1-65535)> { ascii <string> | hex <Hex String> | ipv6 <address> }

no option <code (1-65535)> { ascii <string> |hex <hex_str> | ipv6 <address> }
```

Parameter Description

- `<code(1-65535>` - Indicates a unique option type. This value ranges between 1 and 65535.
- `ascii<string>` - Configures an ASCII string that can be provided as an option value. The maximum string size is 255.
- `hex<Hex String>` - Configures a hexadecimal string that can be provided as an option value. This value is an octet string of size varying between 1 and 32.
- `ipv6 <address>` - Configures an IPv6 address that can be provided as an option value.

Mode

IPv6 DHCP Pool Configuration mode

☞ The DHCPv6 server address pool should be created, before executing this command.

Example

```
Your Product(config-d6pool)# option 30 ipv6 2222::1111
```

Related Command(s)

- `ipv6 dhcp pool`– Creates a DHCP6 server address pool
- `show ipv6 dhcp pool` – Displays the DHCPv6 server pool information

35.3.15 ipv6 dhcp server-id type

Command Objective This command configures the DUID type to be used for the server identifier. DUID consists of a two-octet type code represented in network byte order and a variable number of octets, to make an actual identifier. Server sends a server identifier TLV in the reply message.

Syntax `ipv6 dhcp server-id type {llt | en | ll}`

Parameter Description

- **llt** - Configures the DUID formed based on LLT. The DHCPv6 server uses the link layer address of the interface and current system time value for the server identifier option TLV value. This type of DUID consists of a two octet type field containing the value 1, a two octet hardware type code, four octets containing a time value, and a link-layer address of any one network interface that is connected to the DHCP device at the time of generation of the DUID.
  - For server ID configured as llt, the DHCPv6 client and server should:
    - Compulsorily have a stable storage.
    - Store DUID-LLT in stable storage.
    - Continue to use DUID-LLT, even if network interface used to generate the DUID-LLT is removed.
    - Attempt to configure the time prior to generation of DUID, if possible, and should use time source (For example, real-time clock) for generating the DUID, even if the source is not configurable prior to the generation of the DUID.
- **en** - Configures the DUID which is assigned by the vendor based on EN. The DHCPv6 server uses the vendor-assigned unique ID based on the EN for the server identifier option TLV value. This type of DUID consists of vendor's registered private enterprise number as maintained by IANA and a unique identifier assigned by the vendor.
  - For server ID configured as en:
    - The identifier assigned by the vendor should be unique to device.
    - The unique identifier should be assigned to the device during its manufacture itself and should be stored in a non-volatile storage.
    - The generated DUID should be recorded in a non-erasable storage.
- **ll** - Configures the DUID formed based on LL. The DHCPv6 server uses the link layer address for the server identifier option TLV value. This type of DUID consists of two octets containing the DUID type 3, a two octet network hardware type code, and a link-layer address of any one network interface that is permanently connected to the client or server device.

- For server ID configured as ll:
  - DHCP-LL should not be used by clients or servers that cannot tell whether or not a network interface is permanently attached to the device on which the DHCP client is running.
  - Same DHCP-LL should be used in configuring all network interfaces connected to the device, regardless of usage of any interface's link-layer address to generate the DUID.

Mode IPv6 DHCP Pool Configuration mode

Default llt

☞ The DHCPv6 server address pool should be created, before executing this command.

Example

```
Your Product(config-d6pool)# ipv6 dhcp server-id type en
```

Related Command(s)

- `ipv6 dhcp pool`– Creates a DHCP6 server address pool
- `show ipv6 dhcp pool` – Displays the DHCPv6 server pool information

35.3.16 dhcp server-id interface

Command Objective This command is used to configure the interface that is used in the formation of the DUID based on LLT or on LL.

Syntax `ipv6 dhcp server-id interface <interface-type> <interface-id>`

Parameter Description

- `<interface-type>` - Configures DHCPv6 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.
  - internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Configures DHCPv6 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 internal-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only internal-lan or port-channel ID is provided, for interface types internal-lan and port-channel. For example: 1 represents i-lan and port-channel ID.

Mode IPv6 DHCP Pool Configuration mode

Default An arbitrary interface value is used.

- The DHCPv6 server address pool should be created, before executing this command.
- The physical interface configured to be used in the formation of DUID should have been already configured as router port.

Example

```
Your Product(config-d6pool)# ipv6 dhcp server-id
interface gigabitethernet 0/3
```

Related Command(s)

- `ipv6 dhcp pool` – Creates a DHCP6 server address pool
- `show ipv6 dhcp interface` – Displays the information at server end for specified interface

35.3.17 information refresh

Command Objective

This command configures the refresh time value that is to be sent to the client. The minimum refresh time value that is to be set is 600 seconds (10 minutes).

The no form of the command deletes the refresh timer option from the pool.

Syntax

```
information refresh {days < value integer(0-7) > [hours
< value integer(0-24)> minutes(0-60) < value integer> ]
| infinity}

no information refresh
```

Parameter Description

- `days< value integer(0-7) >` - Configures the refresh time is specified in number of days. The value ranges between 0 and 7.
- `hours< value integer(0-24)>` - Configures the refresh time is specified in number of hours. The value ranges between 0 and 24.
- `minutes(0-60) < value integer>` - Configures the refresh time is specified in number of minutes. The value ranges between 0 and 60.
- `infinity` - Sets IPv6 value of 0xffffffff that is used to configure the information refresh time to infinity. That is, sets the refresh time value as 4294967295 seconds.

Mode

IPv6 DHCP Pool Configuration mode

☞ The DHCPv6 server address pool should be created, before executing this command.

Example

```
Your Product(config-d6pool)# information refresh days
4 hours 5 minutes 56
```

Related Command(s)

- `ipv6 dhcp pool`– Creates a DHCP6 server address pool
- `show ipv6 dhcp pool` – Displays the DHCPv6 server pool information

35.3.18 ipv6 dhcp server

Command Objective

This command associates the DHCPv6 server pool with an interface.

The no form of the command removes the association of the server pool with the interface.

Syntax

```
ipv6 dhcp server [<pool-name (1-64)> [preference
<value (0-255)>]]

no ipv6 dhcp server
```

Parameter Description

- `<pool-name(1-64)>` - Configures the pool name which should be a unique and NULL terminated string.. The naximum string size is 64.
- `preference<value (0-255)>` - Configures the preference value of the pool. This value ranges between 0 and 255.The DHCPv6 client uses this value to select the best information on receiving multiple reply messages from different servers.

Mode

Interface Configuration mode (Vlan / Router)

Default

preference – 0

Example

```
Your Product(config-if)# ipv6 dhcp server 33 preference 45
```

Related Command(s)

- `no switchport` – Configures the port as router port
- `clear ipv6 dhcp server statistics` – Clears DHCPv6 server statistics for a particular interface or for all the interfaces
- `show ipv6 dhcp pool` – Displays the DHCPv6 server pool information
- `show ipv6 dhcp interface` – Displays the various configuration information at server end for specified interface or all the interfaces
- `show ipv6 dhcp server ststistics` – Displays the DHCPv6 server statistics

35.3.19 debug ipv6 dhcp server

Command Objective

This command sets the debugging options and traces in the DHCPv6 server.

The no form of the command unsets the debugging options and traces in the DHCPv6 server, and resets the trace to the default value.

Syntax

```
debug ipv6 dhcp server {[init-shut] [mgmt] [ctrl] [pkt]
 [resource] [fail] [buffer] [critical] | [all]}

no debug ipv6 dhcp server {[init-shut] [mgmt] [ctrl] [pkt]
[resource] [fail] [buffer] [critical] | [all]}
```

Parameter Description

- **init-shut** - Generates debug messages for Init and shutdown traces. These traces are used during the module initialization and shutdown, and for cases such as failure of RBTree creation and so on.
- **mgmt** - Generates debug messages for Management traces.
- **ctrl** - Generates debug messages for Control plane traces. These traces are used for cases such as MBSM card removal, failure of state change and so on.
- **pkt** - Generates debug messages for Packet dump traces. These traces are used during the reception and transmission of packets.
- **resource** - Generates debug messages for Traces related to all resources such as memory, data structure and the like. These traces are used for failure of memory allocation and so on.
- **fail** - Generates debug messages for All failure traces.These traces are used for all valid and invalid failures (expected and unexpected errors).
- **buffer** - Generates debug messages for Buffer allocation / release traces.
- **critical** - Generates debug messages for SL-DHCPv6 server critical traces. These traces are used for cases such as failure of RBTree addition, failure to program the hardware, and so on.
- **all** - Generates debug messages for All traces.

Mode

Privileged Exec Mode / User Exec Mode

Default

critical

Example

```
Your Product# debug ipv6 dhcp server mgmt

D6SR: Trace Option Set enable mgmt
```

35.3.20 clear ipv6 dhcp server statistics

Command Objective This command clears DHCPv6 server statistics for a particular interface or for all the interfaces.

Syntax

```
clear ipv6 dhcp server statistics [interface
{vlan <VlanId(1-4094)> | <interface-type>
<interface-id>} ]
```

Parameter Description

- `vlan<VlanId(1-4094)>` - Clears DHCPv6 server statistics for the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
- `<interface-type> -` Clears DHCPv6 server statisticsfor 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.
  - internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Clears DHCPv6 server statisticsfor 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 Internal-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only internal-lan or port-channel ID is provided, for interface types internal-lan and port-channel. For example: 1 represents internal-lan and port-channel ID.

Mode Privileged Exec Mode

Example

```
Your Product# clear ipv6 dhcp server statistics
```

Related Command(s)

- **ipv6 dhcp server** – Associates the DHCPv6 server pool with an interface
- **show ipv6 dhcp server statistics** – Displays the DHCPv6 server statistics

---

35.3.21 show ipv6 dhcp

Command Objective This command displays the DHCPv6 configuration information at server end.

Syntax `show ipv6 dhcp`

Mode Privileged Exec Mode

Example

```
Your Product# show ipv6 dhcp
Client information:
  Listen UDP port      : 546
  Transmit UDP port : 547
  Sys log status : disabled
  SNMP traps      : none
Server information:
Listen UDP port  : 45
Client Transmit UDP port    : 546
Relay Transmit UDP port     : 547
Sys log status   : enabled
SNMP traps       : auth-fail
Authentication Information:
Client DUID : ers
Realm Name      : 33
Key Value       : 1
Key Identifier : 33:33
Relay information:
Listen UDP port  : 34
Client Transmit UDP port    : 546
Server Transmit UDP port    : 547
Sys log status   : enabled
SNMP traps       : invalid-pkt,max-
hop-count
```

Related Command(s)

- snmp-server enable traps ipv6 dhcp server – Enables the SNMP traps for DHCPv6 server
- ipv6 dhcp server port – Configures the information-request listen, reply transmit and relay-reply transmit UDP ports
- ipv6 dhcp server syslog – Enables or disables the syslog feature in DHCPv6 server
- ipv6 dhcp authentication server client-id – Creates client configuration pool at the server and enters into the client pool configuration mode
- ipv6 dhcp authentication – Configures the realm and key value

35.3.22 show ipv6 dhcp pool

Command Objective This command displays the DHCPv6 server pool information.

Syntax `show ipv6 dhcp pool [<pool-name(1-64)>]`

Parameter Description

- `<pool-name(1-64)>` - Displays the server pool information of the configured pool. This name should be a unique and NULL terminated string.

Mode Privileged Exec Mode

Example

```
Your Product# show ipv6 dhcp pool server-pool1

Pool : server-pool1

ACTIVE

DHCPv6 unique type(DUID Type) : Link-layer Address Plus
Time

DHCPv6 unique identifier(DUID):
000100020000167fe80000000000000020102fff
e030401

Preference : 255

Associated Interfaces : Gi0/3

Associated IPv6 Prefix :

SIP servers      : fe80::200d:88ff:fe67:6666

DNS servers      : fe80::200d:88ff:fe67:6666

SIP domain list : Aricent.com

DNS search list : Aricent.com
```

Related Command(s)

- `ipv6 dhcp pool` – Creates a DHCP6 server address pool
- `vendor-specific` – Enters into vendor-specific configuration mode with vendor-specific identification number
- `link-address` – Sets a link-address IPv6 prefix
- `domain-name` – Defines the DNS domain suffix which is provided to the client in reply message on request

- **dns-server** – Defines the DNS server IP address which is provided to the client in reply message on request
- **sip address** – Defines the SIP server IP address which is provided to the client in reply message on request
- **sip domain-name** – Defines the SIP domain name which is provided to the client in reply message on request
- **option** – Sets pool specific DHCP6 server option
- **ipv6 dhcp server-id** type – Configures the DUID type to be used for the server identifier
- **information refresh** – Configures the refresh time value that is to be sent to the client

35.3.23 show ipv6 dhcp interface

Command Objective This command displays the DHCPv6 configuration information at server end for specified interface or all the interfaces.

Syntax

```
show ipv6 dhcp interface [ {vlan <VlanId(1-4094)>
| <interface-type> <interface-id>}]
```

Parameter Description

- `vlan<VlanId(1-4094)>` - Displays DHCPv6 for the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
- `<interface-type>` - Displays DHCPv6 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>` - Displays DHCPv6 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.

Mode Privileged Exec Mode

Example

```
Your Product# show ipv6 dhcp interface
gigabitethernet 0/3 is in server mode
Preference value : 255
 Using pool : server-pool1
```

Related Command(s)

- `ipv6 dhcp pool` – Creates a DHCP6 server address pool
- `ipv6 dhcp server` – Associates the DHCPv6 server pool with an interface

35.3.24 show ipv6 dhcp server statistics

Command Objective This command displays the DHCPv6 server statistics such as number of PDUs transmitted or received.

Syntax

```
show ipv6 dhcp server statistics [interface {vlan
<VlanId(1-4094)> | <interface-type> <interface-id>} ]
```

Parameter Description

- `vlan<VlanId(1-4094)>` - Displays DHCPv6 server statistics for the specified VLAN ID. This is a unique value that represents the specific VLAN created / to be created. This value ranges between 1 and 4094.
- `<interface-type>` - Displays DHCPv6 server statistics 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.
  - internal-lan – Internal LAN created on a bridge per IEEE 802.1ap.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- `<interface-id>` - Displays DHCPv6 server statistics for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only internal-lan or port-channel ID is provided, for interface types internal-lan and port-channel. For example: 1 represents internal-lan and port-channel ID.

Mode Privileged Exec Mode

Example

```
Your Product# show ipv6 dhcp server statistics
gigabitethernet 0/3
 Transmitted:
```

```
    reply    : 1
    relay-reply : 0
  Received:
    information-request  : 1
    relay-forward  : 0
    invalid   : 0
    hmac-failure    :     0
    lastUnknownTlv :     0
```

Related Command(s)

- **ipv6 dhcp server** – Associates the DHCPv6 server pool with an interface
- **clear ipv6 dhcp server statistics** – Clears DHCPv6 server statistics for a particular interface or for all the interfaces

---

36 RIPv6

RIPv6 functions the same and offers the same benefits as RIP in IPv4. RIP enhancements for IPv6, detailed in RFC 2080, include support for IPv6 addresses and prefixes, and the use of all-RIP-routers multicast group address as the destination address for RIP update messages. RIv6P process maintains a local routing table, referred to as a RIB (Routing Information Database). The RIPv6 RIB contains a set of RIPv6 routes learnt from all its neighboring networking devices.

Before configuring the router to run IPv6 RIP, the ipv6 unicast-routing must be enabled globally, and IPv6 must be enabled on any interface in which IPv6 RIP is to be processed.

The list of CLI commands for the configuration of RIP6 are as follows:

- ipv6 router rip
- ipv6 router rip - name
- ipv6 split-horizon
- ipv6 rip enable
- ipv6 poison reverse
- ipv6 rip default-information originate
- ipv6 rip metric-offset
- redistribute
- redistribute bgp
- distribute prefix
- distribute-list route-map
- distance
- debug ipv6 rip
- show ipv6 rip
- show ipv6 rip stats
- show ipv6 rip filter

36.1 ipv6 router rip

Command Objective

This command enables RIPv6 routing process and enters into the router configuration mode for the RIPv6 routing process.

The no form of the command disables RIPv6 on all VLAN interfaces and router ports.

Syntax

```
ipv6 router rip
no ipv6 router rip
```

Mode

Global configuration mode

☞ This command executes only if IPv6 unicast routing (IPv6 forwarding) is enabled globally.

Example

```
Your Product(config)# ipv6 router rip
```

Related Command(s)

- `ipv6 unicast-routing` - Enables unicast routing.
- `distance` - Enables the administrative distance of the routing protocol and sets the administrative distance value.
- `redistribute` – Enables redistribution of IPv6 prefix from configured protocol into RIPv6.
- `redistribute bgp` – Enables redistribution of IPv6 prefix from configured protocol into RIPv6.
- `distribute prefix` – Enables redistribution of IPV6 prefix from BGP protocol into RIPv6.
- `distribute-list route-map` - Enables route map filtering for inbound or outbound routes.
- `show ipv6 rip` – Displays IPv6 Local RIB and routing protocol information.

36.2 ipv6 router rip - name

Command Objective

This command enables RIPv6 routing process and enters into the router configuration mode for the RIPv6 routing process.

The no form of the command disables RIPv6 on all VLAN interfaces and router ports.

This command is a complete standardized implementation of the existing command and operates similar to that of the command ipv6 router rip.

Syntax

`ipv6 router rip <name>`

`no ipv6 router rip <name>`

Mode

Global configuration mode

☞ This command executes only if IPv6 unicast routing (IPv6 forwarding) is enabled globally.

Example

```
Your Product (config)# ipv6 router rip router1
```

Related Command(s)

- `ipv6 unicast-routing` - Enables unicast routing.
- `distance` - Enables the administrative distance of the routing protocol and sets the administrative distance value.
- `redistribute` – Enables redistribution of IPv6 prefix from configured protocol into RIPv6.
- `redistribute bgp` – Enables redistribution of IPv6 prefix from configured protocol into RIPv6.
- `distribute prefix` – Enables redistribution of IPV6 prefix from BGP protocol into RIPv6.
- `distribute-list route-map` - Enables route map filtering for inbound or outbound routes.
- `show ipv6 rip` – Displays IPv6 Local RIB and routing protocol information.

36.3 ipv6 split-horizon

Command Objective

This command enables the split horizon updates for the RIPv6 which prevents the routing loops in distance routing protocol, by prohibiting the router from advertising a route back onto the interface. The split horizon updates are applied in the response packets sent.

The no form of the command disables the split horizon updates.

Syntax

```
ipv6 split-horizon

no ipv6 split-horizon
```

Mode

Interface configuration mode (VLAN interface / Router port)

Default

Split horizon with poison reverse is enabled

☞ The split horizon updates can be configured, only if the IPv6 processing is enabled. The configuration done is applied for all VLAN interfaces and router ports, in which RIPv6 processing is enabled.

Example

```
Your Product (config-if)# ipv6 split-horizon
```

Related Command(s)

- `ipv6 enable` – Enables IPv6 processing on VLAN interface / switch port that is not configured with an explicit IPv6 address.
- `show ipv6 rip` – Displays IPv6 Local RIB and routing protocol information.

36.4 ipv6 rip enable

Command Objective

This command enables RIPv6 routing process on a VLAN interface / router port.

The no form of the command disables the RIPv6 routing process.

Syntax

```
ipv6 rip enable
no ipv6 rip
```

Mode

Interface configuration mode (VLAN interface / Router port)

☞ The RIPv6 routing process can be configured, only if the IPv6 processing is enabled.

Example

```
Your Product (config-if)# ipv6 rip enable
```

Related Command(s)

- `ipv6 enable` – Enables IPv6 processing on VLAN interface / switch port that is not configured with an explicit IPv6 address.
- `show ipv6 rip` – Displays IPv6 Local RIB and routing protocol information.
- `show ipv6 rip stats` - Displays all the interface statistics related information.
- `show ipv6 rip filter` - Displays the details of the and Advfilter type table.

36.5 ipv6 poison reverse

Command Objective

This command enables poison reverse which informs all routers that the path back to the originating node for a particular packet has an infinite metric. It will advertise that same route out that same interface to that same neighbor. The poison reverse algorithm is applied in the response packets sent.

Syntax

```
ipv6 poison reverse
```

Mode

Interface configuration mode (VLAN interface / Router port)

Default

Poison reverse algorithm is enabled.

☞ The poison reverse algorithm can be configured, only if the IPv6 processing is enabled.

Example

```
Your Product (config-if)# ipv6 poison reverse
```

Related Command(s)

- `ipv6 enable` – Enables IPv6 processing on VLAN interface / switch port that is not configured with an explicit IPv6 address.
- `show ipv6 rip` – Displays IPv6 Local RIB and routing protocol information.

36.6 ipv6 rip default-information originate

Command Objective

This command configures handling of default route originate. This command originates a default IPv6 route into RIP and also forces the advertisement of the route in router updates sent on the interface. The advertisement of the route occurs regardless of whether the route is present in the IPv6 routing table or not.

The routing process ignores all default routes received on any interface, after originating the IPv6 default route out of any interface to avoid routing loops.

The no form of the command disables handling of default route originate.

Syntax

```
ipv6 rip default-information originate

no ipv6 rip default-information
```

Mode

Interface configuration mode (VLAN interface / Router port)

☞ The default route origination can be configured, only if the IPv6 processing is enabled.

Example

```
Your Product (config-if)# ipv6 rip default-information
originate
```

Related Command(s)

- `ipv6 enable` – Enables IPv6 processing on VLAN interface / switch port that is not configured with an explicit IPv6 address.

36.7 ipv6 rip metric-offset

Command Objective

This command sets the IPv6 RIP metric for an interface and adjusts default metric increment. The configured metric value is added before the received IPv6 RIP route before inserting the route into the routing table. Therefore, increasing the IPv6 RIP metric offset of an interface increases the metric value of IPv6 RIP routes received over the interface. The value of the metric offset integer ranges between 1 and 15.

Syntax

```
ipv6 rip metric-offset <integer (1-15)>
```

Mode

Interface configuration mode (VLAN interface / Router port)

☞ This command is used in conjunction with the redistribute command to cause the current routing protocol to use the same metric value for all redistributed routes. The maximum metric that RIP can advertise is 16, and a metric of 16 denotes a route that is unreachable. The metric offset can be configured, only if the IPv6 processing is enabled.

Example

```
Your Product (config-if)# ipv6 rip metric-offset 3
```

Related Command(s)

- `ipv6 enable` – Enables IPv6 processing on VLAN interface / switch port that is not configured with an explicit IPv6 address.

36.8 redistribute

Command Objective

This command enables redistribution of IPv6 prefix from configured protocol into RIPv6. The redistribution is done after applying the route map rule, if the existing route map is specified.

The no form of the command disables redistribution of IPv6 prefix from corresponding protocol into RIPv6. The route map is disassociated for redistribution, if the no form of the command specifies the route map.

Syntax

```
redistribute {static|connected|ospf} metric <integer(0-16)> [route-map <string(20)>]

no redistribute {static|connected|ospf} [route-map <string(20)>]
```

Parameter Description

- `static` - Advertises statically configured routes in the RIPv6 process.
- `connected` - Advertises the connected routes in the RIPv6 process.
- `ospf` - Advertises the OSPF routes in the RIPv6 process.
- `metric<integer(0-16>` - Configures the routing metric associated with the route. This value ranges between 1 and 16.
- `route-map<string(20)>` - Configures the name of the Route Map to be applied during redistribution of routes to RIPv6. If this is not specified, all routes are redistributed. This value is a string with the maximum size as 20.

Mode

RIPv6 Router configuration mode

☞ A route must be advertised with a metric of value 15 or less, as the RIP router always adds an interface cost (default 1) onto the metric of the received route. This makes the metric 16, which denotes that the route is unreachable.

Example

```
Your Product (config-router)# redistribute static metric 6
```

Related Command(s)

- `ipv6 router rip` - Enables RIPv6 routing process and enters into the router configuration mode for the RIPv6 routing process.

- **show ipv6 rip** – Displays IPv6 Local RIB and routing protocol information.

36.9 redistribute bgp

Command Objective

This command redistributes IPv6 prefix from BGP protocol into RIPv6. This command controls redistribution of BGP routes into RIP.

This command has been included to adhere to the Industry Standard CLI syntax. This command is currently not supported (that is, BGP redistribution is not supported).

Syntax

```
redistribute bgp <as-no> [metric <integer(0-16)>]
```

Parameter Description

- `<as-no>` - Configures the autonomous system number that identifies the BGP router to other routers and tags the routing information passed along. This value ranges between 1 and 65535.
- `metric<integer(0-16)>` - Configures the metric to be used for the BGP redistributed routes. This value ranges between 0 and 16.

Mode

RIPv6 Router configuration mode

☞ A route must be advertised with a metric of value 15 or less, as the RIP router always adds an interface cost (default 1) onto the metric of the received route. This makes the metric 16, which denotes that the route is unreachable.

Example

```
Your Product (config-router)# redistribute bgp 10
metric 10
```

Related Command(s)

- `ipv6 router rip` - Enables RIPv6 routing process and enters into the router configuration mode for the RIPv6 routing process.
- `show ipv6 rip` – Displays IPv6 Local RIB and routing protocol information.

36.10 distribute prefix

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.

This distance value will not be used for distribute list. The administrative distance can be enabled for only one route map. The distance should be disabled for the already assigned route map, if distance needs to be enabled 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 existing Route Map for which the distance value should be enabled and set. This value is a string whose maximum size is 20.

Mode

RIPv6 Router configuration mode

Default

120 (Represents RIP route)

Example

```
Your Product (config-router)# distance 10 route-map
rmap-test
```

Related Command(s)

- `ipv6 router rip` - Enables RIPv6 routing process and enters into the router configuration mode for the RIPv6 routing process.
- `show ipv6 rip filter` – Displays peer and Advfilter table.

36.11 distance

Command Objective

This command enables route map filtering for inbound or outbound routes and defines the conditions for distributing the routes from one routing protocol to another.

The route map filtering already enabled for inbound or outbound routes should be disabled, if another route map should be enabled for inbound or outbound routes.

The no form of the command disables route map filtering for inbound or outbound routes.

Syntax

```
distribute-list route-map <name(1-20)> {in | out}
no distribute-list route-map <name(1-20)> {in | out}
```

Parameter Description

- `<name(1-20)>` - Configures the name of the existing Route Map for which filtering should be enabled. This value is a string whose maximum size is 20.
  - `in` - Sets route map filtering for the inbound routes.
  - `out` - Sets route map filtering for the outbound routes.

Mode

RIPv6 Router configuration mode

Example

```
Your Product (config-router)# distribute-list route-map
rmap-test in
```

Related Command(s)

- `ipv6 router rip` - Enables RIPv6 routing process and enters into the router configuration mode for the RIPv6 routing process.

36.12 redistribute bgp

Command Objective

This command redistributes IPv6 prefix from BGP protocol into RIPv6. This command controls redistribution of BGP routes into RIP.

This command has been included to adhere to the Industry Standard CLI syntax. This command is currently not supported (that is, BGP redistribution is not supported).

Syntax

```
redistribute bgp <as-no> [metric <integer(0-16)>]
```

Parameter Description

- `<as-no>` - Configures the autonomous system number that identifies the BGP router to other routers and tags the routing information passed along. This value ranges between 1 and 65535.
- `metric<integer(0-16)>` - Configures the metric to be used for the BGP redistributed routes. This value ranges between 0 and 16.

Mode

RIPv6 Router configuration mode

☞ A route must be advertised with a metric of value 15 or less, as the RIP router always adds an interface cost (default 1) onto the metric of the received route. This makes the metric 16, which denotes that the route is unreachable.

Example

```
Your Product (config-router)# redistribute bgp 10
metric 10
```

Related Command(s)

- `ipv6 router rip` - Enables RIPv6 routing process and enters into the router configuration mode for the RIPv6 routing process.
- `show ipv6 rip` – Displays IPv6 Local RIB and routing protocol information.

36.13 debug ipv6 rip

Command Objective

This command sets debug level for RIPv6 module.

The no form of the command disables debug level for RIPv6 module.

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 ipv6 rip { all | data | control }
no debug ipv6 rip
```

Parameter Description

- `all` - Generates debug messages for all traces.
- `data` - Generates debug messages for Data path traces.
- `control` - Generates debug messages for Control Plane.

Mode

traces Privileged EXEC Mode

Default

Debug level is disabled

Example

```
Your Product# debug ipv6 rip all
```

36.14 show ipv6 rip

Command Objective This command displays information in current IPv6 Local RIB and about RIPv6 routing protocol.

Syntax `show ipv6 rip [ database ]`

Parameter Description

- `database` - Displays the details of the entries in the RIP IPv6 routing table database.

Mode Privileged EXEC Mode

☞ The command displays the RIPv6 details only if the RIPv6 routing process is enabled in any one of the VLAN interface / router port.

Example

```
Your Product# show ipv6 rip database
RIP local RIB
4444::/64, metric 10, local vlan1/::, expires in 180 secs
5555::/64, metric 10, local vlan2/::, expires in 180 secs
6666::/64, metric 7, static tunnel0/::, expires in 180 secs
```

Related Command(s)

- `ipv6 split-horizon` – Enables the split horizon updates for the RIPv6.
- `ipv6 rip enable` – Enables RIPv6 routing process on a VLAN interface / router port.
- `ipv6 poison reverse` – Enables poison reverse.
- `ipv6 rip default-information originate` – Configures handling of default route originate.
- `ipv6 rip metric-offset` – Adjusts default metric increment.
- `redistribute` – Enables redistribution of IPv6 prefix from configured protocol into RIPv6.
- `distribute prefix` – Enables Filter network in routing updates sent or received.
- `debug ipv6 rip` – Enables IPv6 RIP routing protocol debugging.

36.15 show ipv6 rip stats

Command Objective This command displays statistics related information (such as number of requests received) for all VLAN interfaces / router ports in which the RIPv6 routing process is enabled.

Syntax `show ipv6 rip stats`

☞ The command displays the RIPv6 details only if the RIPv6 routing process is enabled in any one of the VLAN interface / router port.

Example

```
Your Product# show ipv6 rip stats
     Interface Index      vlan2000

     ****************     ***

 Rcvd  :

 Messages          0    Requests
 0    Responses     0

 UnknownCommds     0    OtherVer
 0    Discards      0

 Sent  :

 Messages          0    Requests
 0    Responses     0

 Trigger Updates   0
```

Related Command(s)

- `ipv6 rip enable` – Enables RIPv6 routing process on a VLAN interface / router port.

36.16 show ipv6 rip filter

Command Objective This command displays the filtering details (such as filter address) available in the Advfilter type table.

Syntax `show ipv6 rip filter`

Mode Privileged EXEC Mode

☞ The command displays the RIPv6 details only if the RIPv6 routing process is enabled in any one of the VLAN interface / router port.

Example

```
Your Product# show ipv6 rip filter
Filter Address                FilterType
**************                **********
fe80::200:ff:febb:e01         IN
fe80::200:ff:fecc:102         IN
3333::1111                    OUT
```

Related Command(s)

- `distribute prefix` – Enables Filter network in routing updates sent or received.
- `ipv6 rip enable` – Enables RIPv6 routing process on a VLAN interface / router port.

---

37 RRD6

RRD6 (Route Redistribution) allows different routing protocols to exchange IPv6 routing information. [1]

The list of CLI commands for the configuration of RRD6 is as follows:

- export ospfv3
- redistribute-policy – IPv6
- default redistribute-policy – IPv6
- throt
- show redistribute-policy ipv6
- show redistribute information ipv6

[1] Refer to section on RRD (Route Redistribution) for more details on route redistribution.

37.1 export ospfv3

Command Objective	This command enables redistribution of OSPF area/External routes to the protocol. The no form of the command disables redistribution of OSPF area/External routes to the protocol.

Syntax	`export ospfv3 [vrf <vrf-name>] {area-route|external-route} {rip}`
	
	`no export ospfv3 [vrf <vrf-name>] {area-route|external-route} {rip}`

Parameter Description	• `vrf<vrf-name>` - Configures the name of the VRF instance. This value is a string of maximum size 32. This parameter is specific to multiple instance. • `area-route` - Configures redistribution of all OSPFv3 inter-area and intra-area address/mask pairs to be exported into the routing protocol • `external-route` - Configures redistribution of all OSPFv3 Type 1 and Type 2 External address/mask pairs to be exported into the routing protocol • `rip` - Redistributes route information for both internal and external Routing Information Protocol
Mode	Global Configuration Mode
☞	• Router ID must be set for the OSPFv3, before executing this command. • VRF instance should be created, before executing this command to configure the OSPF routes redistribution for the context.
Example	`Your Product (config)# export ospfv3 area-route rip`
Related Command(s)	• `ip vrf` – Creates VRF instance • `show redistribute information ipv6` – Displays the RTM6 RRD status for registered protocols

37.2 redistribute-policy – IPv6

Command Objective	This command adds the IPv6 permit/deny Redistribution Policy. The no form of the command removes the IPv6 permit/deny Redistribution Policy. The addresses learnt within the specified range through the specified routing protocol will be redistributed to other routing protocols. No routes will be exchanged between RTM and the re-distributing protocols

Syntax	`redistribute-policy [vrf <vrf-name>] {ipv6} {permit|deny} <DestIp> <DestRange> {static|local|rip|ospf} {rip|ospf|all}`
	
	`no redistribute-policy [vrf <vrf-name>] {ipv6} <DestIp> <DestRange>`

Parameter Description	• `vrf<vrf-name>` - Configures the name of the VRF instance. This value is a string of maximum size 32. This parameter is specific to multiple instance. • `ipv6` - Configures IPv6 Protocol to which permit/deny Redistribution Policy to be applied. • `permit` - Permits IPv6 Redistribution Policy for all prefixes • `deny` - Denies IPv6 Redistribution Policy for all prefixes • `<DestIp>` - Configures destination IP address for which IPv6 permit/deny Redistribution Policy to be applied • `<DestRange>` - Configures range of destination IP address for which IPv6 permit/deny Redistribution Policy to be applied • `static` - Sets IPv6 permit/deny redistribution policy to Static routes • `local` - Sets IPv6 permit/deny redistribution policy to local Protocol • `rip` - Sets IPv6 permit/deny redistribution policy to Routing Information Protocol • `ospf` - Sets IPv6 permit/deny redistribution policy to Open Shortest Path First Protocol • `all` - Sets IPv6 permit/deny redistribution policy to all protocols
Mode	Global Configuration Mode
Default	• permit all • DestIp -- 0.0.0.0

	• DestRange - 255.255.255.255
Example	`Your Product (config)# redistribute-policy ipv6 permit 4444::1111 64 static ospf`
Related Command(s)	• `ip vrf` – Creates VRF instance • `show redistribute-policy ipv6` – Displays route redistribution filters

37.3 default redistribute-policy – IPv6

Command Objective	This command sets the default behavior of the RRD6 Control Table.
Syntax	`default redistribute-policy [vrf <vrf-name>] {ipv6} {permit | deny}`
Parameter Description	• `vrf<vrf-name>` - Configures the name of the VRF instance. This value is a string of maximum size 32. This parameter is specific to multiple instance. • `ipv6` - Configures IPv6 Protocol to which default redistribution policy to be applied. • `permit` - Permits default redistribution policy for all prefixes • `deny` - Denies default rule for all prefixes
Mode	Global Configuration Mode
Example	`Your Product(config)# default redistribute-policy ipv6 permit`
Related Command(s)	• `ip vrf` – Creates VRF instance • `show redistribute-policy ipv6` – Displays route redistribution filters

37.4 throt

Command Objective	This command configures throt value which is the maximum number of routes processed for every iteration. This value ranges between 1 and 4294967295
Syntax	`throt <value>`
Mode	Global Configuration Mode
Default	1000
Example	`Your Product(config)# throt 100`
Related Command(s)	• `show redistribute information ipv6` – Displays the RTM6 RRD status for registered protocols

37.5 show redistribute-policy ipv6

Command Objective	This command displays IPv6 route redistribution filters.
Syntax	`show redistribute-policy ipv6 [vrf <vrf-name>]`
Parameter Description	• `vrf<vrf-name>` - Displays the name of the VRF instance. This value is a string of maximum size 32. This parameter is specific to multiple instance.
Mode	Privileged EXEC Mode
Example	**Your Product# show redistribute-policy ipv6** VRF Name: default Destination Range SrcProto DestProto Flag ---------- ----- -------- ---------- ---- :: 128 all others Allow VRF Name: vr1 Destination Range SrcProto DestProto Flag ---------- ----- -------- ---------- ---- :: 128 all others Allow **Product # show redistribute-policy ipv6 vrf Your default** VRF Name: default Destination Range SrcProto DestProto Flag ---------- ----- -------- ---------- ---- :: 128 all others Allow
Related Command(s)	• `redistribute-policy-IPv6` – Adds the IPv6 permit/deny Redistribution Policy • `default redistribute-policy ipv6` – Sets the default behavior of the RRD6 Control Table

37.6 show redistribute information ipv6

Command Objective	This command displays the RTM6 RRD status for registered protocols.
Syntax	`show redistribute information ipv6 [vrf <vrf-name>]`
Parameter Description	• `vrf<vrf-name>` - Displays the name of the VRF instance. This value is a string of maximum size 32. This parameter is specific to multiple instance.
Mode	Privileged EXEC Mode
Example	**Your Product# show redistribute information ipv6** Current Throttle Limit: 1000 VRF Name: default Current State is disabled ProtoName OspfAreaRoutes OspfExtRoutes --------- ------------- ------------- local Disable Disable static Disable Disable rip Enable Enable VRF Name: vr1 Current State is disabled ProtoName OspfAreaRoutes OspfExtRoutes --------- ------------- ------------- local Disable Disable static Disable Disable **Your Product# show redistribute information ipv6 vrf default** Current Throttle Limit: 1000 VRF Name: default Current State is disabled ProtoName OspfAreaRoutes OspfExtRoutes --------- ------------- -------------

	local	Disable	Disable
	static	Disable	Disable
	rip	Enable	Enable

Related Command(s)	• `throt` - Configures throt value which is the maximum number of routes processed for every iteration • `export ospfv3` – Enables redistribution of OSPF area/External routes to the protocol

38 IGMP

SMIS IGMP (Internet Group Management Protocol) is a portable implementation of the Internet Group Management Protocol Version 3. It implements the IGMP router functionalities required by the Multicast Routing Protocol.

SMIS IGMP confirms with RFC 3376 for IGMP v3 router functionality. SMIS IGMP supports the MIB defined in draft-ietf-magma-rfc2933-update00.txt.

The deployment of the SMIS IGMP router can be within a routing domain that uses any Multicast Routing Protocol. SMIS IGMP informs MRPs about group membership messages and leave messages.

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

- set ip igmp
- ip igmp immediate-leavel
- ip igmp version
- ip igmp query-interval
- ip igmp query-max-response-time
- ip igmp robustness
- ip igmp last-member-query-interval
- ip igmp static-group
- no ip igmp
- debug ip igmp
- show ip igmp global-config
- show ip igmp interface
- show ip igmp groups
- show ip igmp sources
- show ip igmp statistics
- set backplane interface
- show iftype protocol deny table

38.1 set ip igmp

Command Objective	This command enables or disables IGMP globally or on a particular interface.
Syntax	`set ip igmp {enable|disable}`
Parameter **Description**	• `enable` - Enables IGMP feature globally or on a particular interface. • `disable` - Disables IGMP feature globally or on a particular interface. This removes all dynamic multicast entries, stop all the timers for route entries and disables IGMP on all the IGMP enabled interfaces.
Mode	Global Configuration Mode / Interface Configuration Mode (Vlan/ Router Port)
Default	disable
Example	`Your Product(config)# set ip igmp enable` `Your Product(config-if)# set ip igmp enable`
Related Command(s)	• `ip igmp proxy-service / ip igmp proxy service` Enables IGMP Proxy service in the system. • `show ip igmp global-config` - Displays the global configuration of IGMP.

38.2 ip igmp immediate-leavel

Command Objective	This command enables immediate leave processing on the interface by intimating to the Multicast Routing Protocol on the last member leaving the group. This must be enabled only on those interfaces where there is single host. This feature can also be enabled on those interfaces having more than one hosts only if all are v3 hosts in V3 Mode. The no form of the command disables immediate-leave processing on the interface.

Syntax	`ip igmp immediate-leave`
	
	`no ip igmp immediate-leave`

Mode	Interface Configuration Mode (Vlan/ Router Port)
Default	Immediate leave processing is disabled
Example	`Your Product(config-if)# ip igmp immediate-leave`
Related Command(s)	• `show ip igmp interface` – Displays the interface configuration of IGMP.

38.3 ip igmp version

Command Objective	This command configures the IGMP version on the interface. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN. The no form of the command sets the default IGMP version on the interface.

Syntax	`ip igmp version { 1 | 2 | 3 }`
	
	`no ip igmp version`

Parameter Description	• `1` - Configures the IGMP version 1. • `2` - Configures the IGMP version 2. • `3` - Configures the IGMP version 3.
Mode	Interface Configuration Mode (Vlan/ Router Port)
Default	version 2
Example	`Your Product(config-if)# ip igmp version 1`
Related Command(s)	• `show ip igmp interface` – Displays the interface configuration of IGMP.

38.4 ip igmp query-interval

Command Objective	This command configures the frequency at which IGMP host-query packets are transmitted on the interface. This value ranges between 1 and 65535. The no form of the command resets the IGMP query-interval to its default value.

Syntax	`ip igmp query-interval <value (1-65535) seconds>`
	
	`no ip igmp query-interval`

Mode	Interface Configuration Mode (Vlan/ Router Port)
Default	125 seconds
☞	• Query interval should be greater than 10 for IGMP Version 2 and 3. • Query Interval configuration is not allowed for IGMP Version 1.
Example	`Your Product(config-if)# ip igmp query-interval 30`
Related Command(s)	• `set ip igmp` - Enables or disables IGMP. • `ip igmp version` - Sets the IGMP version on the interface. • `ip igmp query-interval` - Configures the IGMP query interval for the interface. • `show ip igmp interface` - Displays the interface configuration of IGMP.

38.5 ip igmp query-max-response-time

Command Objective	This command configures the maximum IGMP query response value for the interface. This value ranges between 0 and 255. The no form of the command resets the max query response to its default value.

Syntax	`ip igmp query-max-response-time <value (0-255) seconds>`
	
	`no ip igmp query-max-response-time`

Mode	Interface Configuration Mode (Vlan/ Router Port)
Default	100 seconds
☞	This command executes only if query Interval is greater than one tenth of Max Response Time.
Example	`Your Product(config-if)# ip igmp query-max-response-time 20`
Related Command(s)	• `ip igmp query-interval` - Configures the IGMP query interval for the interface. • `show ip igmp interface` - Displays the interface configuration of IGMP. • `show ip igmp groups` - Displays the IGMP groups information.

38.6 ip igmp robustness

Command Objective	This command configures the IGMP robustness value for the interface. This value ranges between 1 and 255. The robustness variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the robustness value may be increased. The no form of the command resets the robustness value to its default value.

Syntax	`ip igmp robustness <value(1-255)>`
	
	`no ip igmp robustness`

Mode	Interface Configuration Mode (Vlan/ Router Port)
Default	2
Example	`Your Product(config-if)# ip igmp robustness 100`
Related Command(s)	• `show ip igmp interface` – Displays the interface configuration of IGMP.

38.7 ip igmp last-member-query-interval

Command Objective	This command configures the IGMP last member query interval for the interface. The last member query interval is the maximum response time inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. This value is tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This value ranges between 0 and 255. The no form of the command sets the last member query interval to its default value.

Syntax	`ip igmp last-member-query-interval <value(0-255)>`
	
	`no ip igmp last-member-query-interval`

Mode	Interface Configuration Mode (Vlan/ Router Port)
Default	10
☞	This command executes only if the igmp version on this interface is set to 2 or 3.
Example	`Your Product(config)# ip igmp last-member-query-interval 100`
Related Command(s)	• `set ip igmp` - Enables or disables IGMP. • `ip igmp version` - Sets the IGMP version on the interface. • `ip igmp immediate-leave` - Enables immediate leave processing on the interface. • `show ip igmp interface` - Displays the interface configuration of IGMP.

38.8 ip igmp static-group

Command Objective

This command adds the static group membership on the interface.

The no form of the command deletes the static group membership on the interface.

Syntax

```
ip igmp static-group <Group Address> [source <Source Address>]

no ip igmp static-group <Group Address>
[source <Source Address>]
```

Parameter Description

- `<Group Address>` - Configures the group IP address as a static group member on the interface.
- `source<Source Address>` - Configures the source IP address of a system where multicast data packets originate.

Mode

Interface Configuration Mode (Vlan/ Router Port)

☞

The igmp version on the interface must be set to 3 for configuring static group along with source information.

Example

```
Your Product(config-if)# ip igmp static-group
224.1.2.3 source 12.0.0.1
```

Related Command(s)

- `set ip igmp` – Enables or disables IGMP.
- `ip igmp version` - Sets the IGMP version on the interface.
- `show ip igmp groups` – Displays the IGMP groups information.
- `show ip igmp sources` – Displays the IGMP sources information.
- `show ip igmp interface` – Displays the interface configuration of IGMP.

38.9 no ip igmp

Command Objective	This command deletes the IGMP capable interface; i.e disables IGMP feature in a particular interface. At least one of the interface configuration commands must have been executed to create the IGMP interface.
Syntax	`no ip igmp`
Mode	Interface Configuration Mode (Vlan/ Router Port)
Example	`Your Product(config-if)# no ip igmp`
Related Command(s)	• `show ip igmp interface` - Displays the interface configuration of IGMP.

38.10 debug ip igmp

Command Objective	This command enables the tracing of the IGMP 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 IGMP module as per the configured debug levels. The trace statements are not generated for the configured trace levels.

Syntax	`debug ip igmp ( [i/o][grp][qry][tmr][mgmt] [all] )`
	
	`no debug ip igmp ( [i/o][grp][qry][tmr][mgmt] [all] )`

Parameter **Description**	• `i/o` - Generates debug statements for input/ output traces. • `grp` - Generates debug statements for group related traces. • `qry` - Generates debug statements for query related traces. • `tmr` - Generates debug statements for timer related traces.. • `mgmt` - Generates debug statements for management configuration traces. • `all` - Generates debug statements for all kinds of traces.
Mode	Privileged EXEC Mode
Default	Tracing of the IGMP module is disabled.
Example	`Your Product# debug ip igmp all`

38.11 show ip igmp global-config

Command Objective	This command displays the global configuration of IGMP.
Syntax	`show ip igmp global-config`
Mode	Privileged EXEC Mode
Example	`Your Product(config)# show ip igmp global-config` `IGMP is globally enabled`
Related Command(s)	• `set ip igmp` - Enables or disables IGMP. • `ip igmp proxy-service / ip igmp proxy service` - Enables IGMP Proxy service in the system.

38.12 show ip igmp interface

Command Objective This command displays the interface configuration of IGMP.

Syntax

```
show ip igmp interface [{ Vlan <vlan-id> | <vlan-id/vfiid> <interface-id> | <IP-interface-type> <IP-interfacenumber> }]
```

Parameter

Description

- `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.

    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 IGMP Interface configuration 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>** - Displays IGMP Interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan and port-channel ID is provided, for interface types i-lan and portchannel. For example: 1 represents i-lan and port-channel ID.
- **<IP-interface-type>** - Display IGMP interface configuration for the specified L3 Psuedo wire interface in the system.
- **<IP-interface-number>** - Display IGMP interface configuration 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 Privileged EXEC Mode

Example

```
Your Product# show ip igmp interface
vlan1, line protocol is up
  Internet Address is 10.0.0.1/8
  IGMP is enabled on interface
  Current IGMP router version is 2
  IGMP query interval is 125 seconds
  Last member query response interval is 10 seconds
IGMP max query response time is 100 seconds
  Robustness value is 2
  IGMP querying router is 10.0.0.1 (this system)
```

```
  Fast leave is disabled on this interface
  No multicast groups joined
vlan2, line protocol is up
  Internet Address is 20.0.0.1/8
  IGMP is enabled on interface
  Current IGMP router version is 2
  IGMP query interval is 125 seconds
  Last member query response interval is 10 seconds
IGMP max query response time is 100 seconds
  Robustness value is 2
  IGMP querying router is 20.0.0.1 (this system)
  Fast leave is disabled on this interface
  No multicast groups joined
```

Related Command(s)

- **set ip igmp** - Enables or disables IGMP.
- **ip igmp immediate-leave** - Enables immediate leave processing on the interface.
- **ip igmp version** - Sets the IGMP version on the interface.
- **ip igmp query-interval** - Sets the IGMP query interval for the interface.
- **ip igmp query-max-response-time** - Sets the IGMP max query response value for the interface.
- **ip igmp robustness** - Sets the IGMP robustness value for the interface.
- **ip igmp last-member-query-interval** - Sets the IGMP last member query interval for the interface.
- **ip igmp static-group** - Adds the static group membership on the interface.

38.13 show ip igmp groups

Command Objective This command displays the IGMP groups information.

Syntax

```
show ip igmp groups
```

Mode Privileged EXEC Mode

Example

```
Your Product(config)# show ip igmp groups
I - Include Mode,   E - Exclude Mode
S - Static Mbr,     D - Dynamic Mbr
GroupAddress   Flg Iface    UpTime     ExpiryTime    LastReporter
--------------- ------- ---------------------- -----------
224.5.5.5      S    vlan2   [0d 00:00:22.28] [0d 00:00:00.00] 20.0.0.1
226.7.7.7      IS   vlan3   [0d 00:00:04.59] [0d 00:00:00.00] 30.0.0.1
```

Related Command(s)

- `ip igmp static-group` - Adds the static group membership on the interface.
- `ip igmp version` - Sets the IGMP version on the interface.

38.14 show ip igmp sources

Command Objective This command displays the IGMP source information.

Syntax `show ip igmp sources`

Mode Privileged EXEC Mode

Example

```
Your Product(config)# show ip igmp sources
I - Include Mode,  E - Exclude Mode
S - Static Mbr,    D - Dynamic Mbr
F - Forward List, N - Non-Forward List
GroupAddress  Iface  SrcAddress  Flg  ExpiryTime  LastReporter
--------------- ------- ---------------------- -----------
226.7.7.7    vlan3   12.0.0.1   ISF  [0d 00:00:00.00] 30.0.0.1
```

Related Command(s)

- `ip igmp static-group` - Adds the static group membership on the interface.
- `ip igmp version` - Sets the IGMP version on the interface.

38.15 show ip igmp statistics

Command Objective This command displays the IGMP statistics information.

Syntax

```
show ip igmp statistics [{ Vlan <vlan-id/vfi-id> |
<interface-type> <interface-id> | <IP-interface-
type> <IP-interface-number>}]
```

Parameter

Description

- `Vlan <vlan-id/vfi-id>` - Displays IGMP statistics 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.

- `<interface-type>` - Displays the IGMP statistics information 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>** - Displays IGMP statistics information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than i-lan and port-channel. For example: 0/1 represents that the slot number is 0 and port number is 1. Only i-lan and port-channel ID is provided, for interface types i-lan and portchannel. For example: 1 represents i-lan and port-channel ID.

- **<IP-interface-type>** - Display IGMP statistics information for the specified L3 Psuedo wire interface in the system.

- **<IP-interface-number>** - Display IGMP statistics 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.

Mode Privileged EXEC Mode

Example

```
Your Product# show ip igmp interface
IGMP Statistics for vlan1
  Number of General queries received 1
  Number of Group Specific queries received 0
  Number of Group and Source Specific queries received 0
  Number of v1/v2 reports received 0
  Number of v3 reports received 8
  Number of v2 leaves received 0
  Number of General queries transmitted 1
```

```
  Number of Group Specific queries transmitted 1

  Number of Group and Source Specific queries
transmitted 2

    IGMP Statistics for vlan3

  Number of General queries received 0

  Number of Group Specific queries received 0

  Number of Group and Source Specific queries received 0

  Number of v1/v2 reports received 0

  Number of v3 reports received 6

  Number of v2 leaves received 0

  Number of General queries transmitted 1

  Number of Group Specific queries transmitted 0

  Number of Group and Source Specific queries
transmitted 0
```

Related Command(s)

- **ip igmp static-group** - Adds the static group membership on the interface.
- **ip igmp version** - Sets the IGMP version on the interface.

38.16 set backplane interface

Command Objective	This command configures an interface as backplane interface in the system.
Syntax	`set backplane interface` `no set backplane interface`
Mode	Interface Configuration Mode (Physical)
Example	`Your Product(config-if)# set backplane interface`

38.17 show iftype protocol deny table

Command Objective	This commad displays the entries of iftype protocol deny table.
Syntax	`show iftype protocol deny table [switch <context_name>]`
Parameter Description	• `switch <context_name>` - Displays the iftype protocol denty table entries 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(config)# show iftype protocol deny table
Switch default
IfType                BridgePortType        Protocol
-----------------------------------------------------
Pip                   PropCustomerEdgePortlldp
Pip                   PropCustomerEdgePortqos
Pip                   CustomerBackbonePortecfm
Pip                   CustomerBackbonePortbridge
```

39 PIM

PIM (Protocol Independent Multicast) is a multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. Multicast IP Routing protocols are used to distribute data to multiple recipients. Using multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients. A multicast group identifies a set of recipients that are interested in a particular data stream, and is represented by an IP address from a well-defined range. Data sent to this IP address is forwarded to all members of the multicast group.

PIM is independent of unicast routing protocol and can be operated in two modes: dense and sparse. It is designed to provide scalable inter-domain multicast routing across the Internet. PIM provides multicast routing and forwarding capability to the switch. It maintains the integrity of the hardware based multicast forwarding table with respect to the forwarding table existing in the software. It is independent of the underlying unicast routing protocol and uses the information from the Unicast Routing protocol.

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

- set ip pim graft-retry interval
- no ip pim interface
- debug ip pim
- show ip pim interface
- show ip pim neighbor
- show ip pim rp-candidate
- show ip pim rp-set
- show ip pim bsr
- show ip pim rp-static
- show ip pim component
- show ip pim thresholds
- show ip pim mroute
- show ip pim redundancy state
- show ip pim redundancy shadow-table
- ip pim bsr-border
- set ip pim rpf vector
- show ip pim rp-hash

39.1 set ip pim

Command Objective	This command globally enables / disables PIM feature in the switch.
Syntax	`set ip pim {enable|disable}`
Parameter Description	• `enable` - Enables PIM feature in the switch. • `disable` - Disables PIM feature in the switch.
Mode	Global Configuration Mode
Default	Disable
☞	IGMP proxy service must be disabled in the system, before enabling the PIM globally.
Example	`Your Product(config)# set ip pim enable`
Related Command(s)	• `no ip igmp proxy-service` - Disables IGMP Proxy service in the system. • `set ip pim graft-retry interval` - Configures the time before which graft is retransmitted upon no receipt of Graft ACK. • `set ip pim lan-prune-delay` - Enables / disables the LanPruneDelay bit configured for the router interface to advertise the Lan delay. • `ip pim lan-delay` - Configures the LanDelay configured for the router interface. • `ip pim override-interval` – Configures the override interval configured for router interface. • `ip pim dr-priority` - Configures the designated router priority value configured for the router interface. • `ip pim componentId` - Adds the interface to the PIM component. • `ip pim bsr-candidate – value / ip pim bsr-candidate – vlan` - Configures the local interface as a candidate Bootstrap Router.

- **ip pim message-interval** - Configures the frequency at which PIM Join/ Prune messages are transmitted on the PIM interface.
- **ip pim query-interval** - Configures the frequency at which PIM hello messages are transmitted on this interface.
- **rp-static rp-address** - Configures the address of the interface, which will be advertised as a Static-RP.
- **rp-candidate holdtime** - Configures the holdtime of the component when it is a candidate RP in the local domain.
- **rp-candidate rp-address** - Configures the address of the interface, which will be advertised as a Candidate-RP.
- **set mode** - Sets the component mode to sparse or dense.
- **set ip pim source-active interval** - Configures the time duration for which the SRM control messages would be originated by the router after a data packet is received.
- **ip pim state-refresh disable** - Disables the SRM processing and forwarding.
- **set ip pim state-refresh origination-interval** - Configures the interval between successive SRM (State Refresh Messages) control messages originated and sent out by the router.
- **set ip pim static-rp** - Enables or disables the Static RP configuration Status.
- **ip pim component** - Configures the PIM component in the router and enters into pim component mode.
- **set ip pim pmbr** - Enables or disables the PIM Multicast Border Router (PMBR) Status.
- **set ip pim regstop-ratelimit-period** - Configures the period over which RP monitors the number of register packets after sending the register stop message.
- **set ip pim rp-switchperiod** - Configures the time period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree.
- **set ip pim rp-threshold** - Configures the threshold at which the RP (Rendezvous Point) initiates switching to source specific shortest path tree.
- **set ip pim spt-switchperiod** - Configures the time period (in seconds) over which the data rate is to be monitored for switching to shortest path tree.
- **set ip pim threshold** - Configures the Shortest Path Tree (SPT) group or source threshold.
- **show ip pim mroute** - Displays the PIM multicast information.
- **show ip pim thresholds** - Displays the threshold configured for SPT, RP thresholds, and rate limit values for both SM.

- **show ip pim component** - Displays the component information. The component ID value ranges between 1 and 255.
- **show ip pim rp-static** - Displays the static RP information.
- **show ip pim bsr** - Displays the BSR information.
- **show ip pim rp-set** - Displays the RP-set information.
- **show ip pim rp-candidate** - Displays the candidate RP information.
- **show ip pim neighbor** - Displays the router's PIM neighbors' information.
- **show ip pim interface** - Displays the router's PIM interfaces.
- **debug ip pim** - Enables the tracing of the PIM module as per the configured debug levels.
- **no ip pim interface** - Deletes an interface at PIM level.
- **show ip pim rp-hash** - Displays the elected RP for the multicast group address with the mask length.

39.2 ip multicast

Command Objective	This command globally enables PIM feature in the switch. This command is a standardized implementation of the existing command; set ip pim. It operates similar to the existing command.
Syntax	`ip multicast`
Mode	Global Configuration Mode
Default	PIM feature is disabled in the switch.
☞	IGMP proxy service must be disabled in the system, before enabling the PIM globally.
Example	`Your Product(config)# ip multicast`
Related Command(s)	• `no ip igmp proxy-service` - Disables IGMP Proxy service in the system. • `set ip pim graft-retry interval` - Configures the time before which graft is retransmitted upon no receipt of Graft ACK. • `set ip pim lan-prune-delay` - Enables / disables the LanPruneDelay bit configured for the router interface to advertise the Lan delay. • `ip pim lan-delay` - Configures the LanDelay configured for the router interface. • `ip pim override-interval` – Configures the override interval configured for router interface. • `ip pim dr-priority` - Configures the designated router priority value configured for the router interface.

- **ip pim componentId** - Adds the interface to the PIM component.
- **ip pim bsr-candidate – value / ip pim bsr-candidate – vlan** - Configures the local interface as a candidate Bootstrap Router.
- **ip pim message-interval** - Configures the frequency at which PIM Join/ Prune messages are transmitted on the PIM interface.
- **ip pim query-interval** - Configures the frequency at which PIM hello messages are transmitted on this interface.
- **rp-static rp-address** - Configures the address of the interface, which will be advertised as a Static-RP.
- **rp-candidate holdtime** - Configures the holdtime of the component when it is a candidate RP in the local domain.
- **rp-candidate rp-address** - Configures the address of the interface, which will be advertised as a Candidate-RP.
- **set mode** - Sets the component mode to sparse or dense.
- **set ip pim source-active interval** - Configures the time duration for which the SRM control messages would be originated by the router after a data packet is received.
- **ip pim state-refresh disable** - Disables the SRM processing and forwarding.
- **set ip pim state-refresh origination-interval** - Configures the interval between successive SRM (State Refresh Messages) control messages originated and sent out by the router.
- **set ip pim static-rp** - Enables or disables the Static RP configuration Status.
- **ip pim component** - Configures the PIM component in the router and enters into pim component mode.
- **set ip pim pmbr** - Enables or disables the PIM Multicast Border Router (PMBR) Status.
- **set ip pim regstop-ratelimit-period** - Configures the period over which RP monitors the number of register packets after sending the register stop message.
- **set ip pim rp-switchperiod** - Configures the time period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree.
- **set ip pim rp-threshold** - Configures the threshold at which the RP (Rendezvous Point) initiates switching to source specific shortest path tree.

- **set ip pim spt-switchperiod** - Configures the time period (in seconds) over which the data rate is to be monitored for switching to shortest path tree.
- **set ip pim threshold** - Configures the Shortest Path Tree (SPT) group or source threshold.
- **show ip pim mroute** - Displays the PIM multicast information.
- **show ip pim thresholds** - Displays the threshold configured for SPT, RP thresholds, and rate limit values for both SM.
- **show ip pim component** - Displays the component information. The component ID value ranges between 1 and 255.
- **show ip pim rp-static** - Displays the static RP information.
- **show ip pim bsr** - Displays the BSR information.
- **show ip pim rp-set** - Displays the RP-set information.
- **show ip pim rp-candidate** - Displays the candidate RP information.
- **show ip pim neighbor** - Displays the router's PIM neighbors' information.
- **show ip pim interface** - Displays the router's PIM interfaces.
- **debug ip pim** - Enables the tracing of the PIM module as per the configured debug levels.
- **no ip pim interface** - Deletes an interface at PIM level.
- **show ip pim rp-hash** - Displays the elected RP for the multicast group address with the mask length.

39.3 ip pim version

Command Objective	This command configures version number of the PIM protocol in the switch. 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	`ip pim version { 1 | 2 }`
Parameter **Description**	• `1` - Configures the version as PIM version 1. In PIMv1 , the range of supported multicast groups can be limited with an Access Control List (ACL). PIM version 1 is currently not supported. • `2` - Configures the version as PIM version 2. PIMv2 provides a standards-compliant equivalent to Auto-RP, called the bootstrap router method.
Mode	Global Configuration Mode
Default	PIM Version - 2
Example	`Your Product(config)# ip pim version 2`
Related Command(s)	• `show ip pim component` - Displays the component information. • `show ip pim interface` - Displays the router's PIM interfaces.

39.4 set ip pim threshold

Command Objective	This command configures the Shortest Path Tree (SPT) group or source threshold. To switch to SPT, the threshold must be configured.
Syntax	`set ip pim threshold { spt-grp | spt-src } < number of packets(0-2147483647)>`
Parameter **Description**	• `spt-grp` - Initiates the source specific counters for a particular group when the threshold of data rate for any group exceeds. It is based on number of packets. • `spt-src` - Initiates the switching to shortest path tree when the threshold of data rate for any source exceeds. It is based on number of packets. • `< number of packets(0-2147483647)>` - Specifies the number of registered packets received. This value ranges between 0 and 2147483647.
Mode	Global Configuration Mode
Default	0
☞	This command executes only if PIM / PIMv6 module is enabled globally.
Example	`Your Product(config)# set ip pim threshold spt-grp 50`

Related Command(s)

- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `set ipv6 pim` - Enables / disables PIMv6 feature in the switch globally.
- `set ip pim spt-switchperiod` - Configures the time period (in seconds) over which the data rate is to be monitored for switching to shortest path tree.
- `show ip pim thresholds` - Displays threshold configured for SPT, RP thresholds, rate limit values for both SM.

39.5 set ip pim spt-switchperiod

Command Objective	This command configures the time period (in seconds) over which the data rate is to be monitored for switching to shortest path tree. This value ranges between 0 and 2147483647. The same period is used for monitoring the data rate for both source and group. To switch to SPT, this period must be configured. The SPT is used for multicast transmission of packets with the shortest path from sender to recipients.
Syntax	`set ip pim spt-switchperiod <0-2147483647(in secs)>`
Mode	Global Configuration Mode
Default	0 seconds

☞ This command executes only if PIM / PIMv6 module is enabled globally.

Example

```
Your Product(config)# set ip pim spt-switchperiod 60
```

Related Command(s)

- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `set ipv6 pim` - Enables / disables PIMv6 feature in the switch globally.
- `show ip pim thresholds` - Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM.

39.6 set ip pim rp-threshold

Command Objective	This command configures the threshold at which the RP (Rendezvous Point) initiates switching to source specific shortest path tree. This value ranges between 0 and 214748364. To switch to SPT, this threshold must be configured and the switching is based on the number of registered packets received.
Syntax	`set ip pim rp-threshold <0-2147483647(number of reg packets)>`
Mode	Global Configuration Mode
Default	0
☞	This command executes only if PIM / PIMv6 module is enabled globally.
Example	`Your Product(config)# set ip pim rp-threshold 50`
Related Command(s)	• `set ip pim / ip multicast` - Enables or disables the PIM globally. • `set ipv6 pim` - Enables / disables PIMv6 feature in the switch globally. • `show ip pim thresholds` - Displays threshold configured for SPT, RP thresholds, rate limit values for both SM and DM.

39.7 set ip pim rp-switchperiod

Command Objective	This command configures the time period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree. This value ranges between 0 and 2147483647. RP-tree is a pattern that multicast packets are sent to a PIM-SM router by unicast and then forwarded to actual recipients from RP. To switch to SPT, this period must be configured.
Syntax	`set ip pim rp-switchperiod <0-2147483647(in secs)>`
Mode	Global Configuration Mode
Default	0 seconds

☞ This command executes only if PIM / PIMv6 module is enabled globally.

Example

```
Your Product(config)# set ip pim rp-switchperiod 100
```

Related Command(s)

- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `set ipv6 pim` - Enables / disables PIMv6 feature in the switch globally.
- `show ip pim thresholds` - Displays threshold configured for SPT, RP thresholds, rate limit values for both SM.

39.8 set ip pim regstop-ratelimit-period

Command Objective	This command configures the period over which RP monitors the number of register packets after sending the register stop message. This value ranges between 0 and 2147483647. Register stop message is used to avoid encapsulation of multicast data packets from the first hop router to the RP.
Syntax	`set ip pim regstop-ratelimit-period <0-2147483647(in secs)>`
Mode	Global Configuration Mode
Default	5 seconds
☞	This command executes only if PIM / PIMv6 module is enabled globally.
Example	`Your Product(config)# set ip pim regstop-ratelimit-period 100`
Related Command(s)	• `set ip pim / ip multicast` - Enables or disables the PIM globally. • `set ipv6 pim` - Enables / disables PIMv6 feature in the switch globally. • `show ip pim thresholds` - Displays threshold configured for SPT, RP thresholds, rate limit values for both SM.

39.9 set ip pim pmbr

Command Objective	This command enables or disables the PIM Multicast Border Router (PMBR) Status. A PMBR integrates two different PIM domains (either PIM -SM or PIM -DM) and also connects a PIM domain to other multicast routing domain(s).
Syntax	`set ip pim pmbr { enable | disable }`
Parameter Description	• **enable** - Enables the PMBR Status. • **disable** - Disables the PMBR Status.
Mode	Global Configuration Mode
Default	disable
☞	This command executes only if PIM / PIMv6 module is enabled globally.
Example	`Your Product(config)# set ip pim pmbr enable`
Related Command(s)	• **set ip pim / ip multicast** - Enables or disables the PIM globally. • **set ipv6 pim** - Enables / disables PIMv6 feature in the switch globally. • **show ip pim thresholds** - Displays threshold configured for SPT, RP thresholds, rate limit values for both SM.

39.10 ip pim component

Command Objective

This command configures the PIM component in the router and enters into pim component mode. The PIM component corresponds to each instance of a PIM domain and classifies it as Sparse or Dense mode.

The no form of the command destroys the PIM component. This value ranges between 2 and 255.

Syntax

```
ip pim component <ComponentId (1-255)> [Scope-zonename(64)]

no ip pim component <ComponentId (2-255)>
```

Parameter Description

- `<ComponentId (1-255)>` - Configures the PIM component in the router and enters into pim component mode. This value ranges between 1 and 255.
- `Scope-zone-name(64)` - Configures the scope-zone-name. The maximum length of the string is 64. To configure the scope-zone name, scope-zone should be created in the interface. Scope is a 4-bit value that describes the scope of an IPV6 address. A unicast address can possibly have 2 scopes (Linklocal and Global) only and a multicast address can have a maximum of 11 scopes. The scope zone name should be the same as that of the zone created in the ipv6 scope zone command. If ipv6 scopezone is created as scopeA 1, then the scope zone name should be scopeA1. (Without space).

Mode

Global Configuration Mode

Default

Component-Id - 1

☞ This command executes only if PIM / PIMv6 module is enabled globally.

Example

```
Your Product(config)# set ip pim pmbr enable

Your Product (pim-comp)#
```

Related Command(s)

- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `set ipv6 pim` - Enables / disables PIMv6 feature in the switch globally.
- `ipv6 scope-zone` - Creates IPv6 scope zone on an interface.
- `show ip pim component` - Displays the component information.
- `set ip pim graft-retry interval` - Configures the time before which graft is retransmitted upon no receipt of Graft ACK.
- `set ipv6 pim graft-retry interval` - Configures the time before which graft is retransmitted upon no receipt of Graft ACK.

39.11 set ip pim static-rp

Command Objective

This command enables or disables the Static RP configuration Status. This command specifies whether to use the configured static- RP.

Syntax

```
set ip pim static-rp { enable | disable }
```

Parameter Description

- `enable` - Enables the Static RP configuration status.
- `disable` - Disables the Static RP configuration status.

Mode

Global Configuration Mode

Default

Disable

☞ This command executes only if PIM / PIMv6 module is enabled globally.

Example

```
Your Product(config)# set ip pim static-rp enable
```

Related Command(s)

- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `set ipv6 pim` - Enables / disables PIMv6 feature in the switch globally.
- `show ip pim rp-set` - Displays the RP-set information.
- `show ip pim rp-static` - Displays the RP-static information.

39.12 set ip pim state-refresh origination-interval

Command Objective	This command configures the interval between successive SRM (State Refresh Messages) control messages originated and sent out by the router. This value ranges between 4 and 100. The no form of the command disables origination (generation) of SRM control messages by the router. This command is useful if the router is the First-hop router, that is, the source is directly connected

Syntax	`set ip pim state-refresh origination-interval [<4-100>]`
	
	`no ip pim state-refresh origination-interval`

Mode	Global Configuration Mode
Default	60 seconds

☞ This command executes only if PIM / PIMv6 module is enabled globally.

Example

```
Your Product(config)# set ip pim state-refresh
origination-interval 5
```

Related Command(s)

- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `set ipv6 pim` - Enables / disables PIMv6 feature in the switch globally.
- `show ip pim interface detail` - Displays the router's PIM interfaces.

39.13 ip pim state-refresh disable

Command Objective

This command disables the SRM processing and forwarding, that is, the router drops the State Refresh Messages, if received and also the router will not advertise the SR Capability in Hello messages.

The no form of the command enables the SRM processing and forwarding. On enabling, this router advertises itself as SR Capable in Hello Messages.

Syntax

```
ip pim state-refresh disable

no ip pim state-refresh disable
```

Mode

Global Configuration Mode

Default

SRM processing and forwarding is enabled.

☞ This command executes only if PIM / PIMv6 module is enabled globally.

Example

```
Your Product(config)# ip pim state-refresh disable
```

Related Command(s)

- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `set ipv6 pim` - Enables / disables PIMv6 feature in the switch globally.
- `show ip pim interface detail` - Displays the router's PIM interfaces.

39.14 set ip pim source-active interval

Command Objective	This command configures the time duration for which the SRM control messages would be originated by the router after a data packet is received. The no form of the command sets the source active interval to its default value. This command is useful if the router is the First-hop router, that is, the source is directly connected.

Syntax	`set ip pim source-active interval <120-210>`
	
	`no ip pim source-active interval`

Mode	Global Configuration Mode
Default	210 seconds.
☞	This command executes only if PIM / PIMv6 module is enabled globally.
Example	`Your Product(config)# set ip pim source-active interval 150`
Related Command(s)	• `set ip pim / ip multicast` - Enables or disables the PIM globally. • `set ipv6 pim` - Enables / disables PIMv6 feature in the switch globally. • `show ip pim mroute` - Displays the PIM multicast information.

39.15 set mode

Command Objective	This command sets the component mode to sparse or dense.
Syntax	`set mode {sparse | dense}`
Parameter **Description**	• `sparse` - Indicates the component is running in Sparse mode, explicitly building unidirectional shared trees rooted at a rendezvous point (RP) per group, and optionally creates shortest-path trees per source. • `dense` - Indicates the component is running in Dense mode, implicitly building shortest-path trees by flooding multicast traffic domain wide, and then pruning back branches of the tree where no receivers are present.
Mode	PIM Component Mode
Default	sparse
☞	This command executes only if PIM / PIMv6 module is enabled globally.
Example	`Your Product(pim-comp)# set mode dense`
Related Command(s)	• `set ip pim / ip multicast` - Enables or disables the PIM globally. • `set ipv6 pim` - Enables / disables PIMv6 feature in the switch globally. • `ip pim component` - Configures the PIM component in the router and enters into pim component mode. • `set ip pim graft-retry interval` - Configures the time before which graft is retransmitted upon no receipt of Graft ACK. • `set ipv6 pim graft-retry interval` - Configures the time before which graft is retransmitted upon no receipt of Graft ACK. • `show ip pim component` - Displays the component information.

39.16 rp-candidate rp-address

Command Objective

This command configures the address of the interface, which will be advertised as a Candidate-RP.

A Candidate-RP is a router configured to send periodic Candidate-RPAdvertisement messages to the BSR, and processes Join/Prune or Register messages for the advertised group prefix, when it is elected as RP.

The no form of the command disables the address of the interface, which will be advertised as a Candidate-RP

Syntax

```
rp-candidate rp-address <Group Address> <Group Mask>
<IP address> [Priority <0-255>]

no rp-candidate rp-address <Group Address> <Group
Mask> <RP address>
```

Parameter Description

- `<Group Address>` - Configures the IP multicast group address for which the entry contains multicast routing information.
- `<Group Mask>` - Configures the IP multicast group address mask that, gives the group prefix for which the entry contains information about the RP.
- `<IP address>` - Configures the IP address.
- `Priority <0-255>` - Configures the priority of the candidate RP. This value ranges between 0 and 255.

Mode

PIM Component Mode

☞

This command executes only if

- PIM module is enabled globally.
- PIM mode is set as sparse.
- PIM query interval and IP address is configured.

Example

```
Your Product(pim-comp)# rp-candidate rp-address
224.1.0.0 255.255.0.0  20.0.0.2
```

Related Command(s)

- `set ip pim / ip multicast` - Enables or disables the PIM globally.
- `set mode` - Sets the component mode to sparse or dense.
- `ip address` - Sets the IP address for an interface.
- `ip pim component` - Configures the PIM component in the router and enters into pim component mode.
- `ip pim componentId` - Adds the interface to the PIM component.
- `ip pim query-interval` – Configures the frequency at which PIM hello messages are transmitted on the interface .
- `ip pim bsr-candidate - value` – Sets the preference value for the local interface as a candidate bootstrap router.
- `ip pim bsr-candidate – VLAN` – Sets the local interface as a candidate bootstrap router.
- `show ip pim interface` – Displays the router's PIM interfaces.
- `show ip pim rp-set` – Displays the RP-set information .
- `show ip pim rp-candidate`– Displays the RP-candidate information.
- `show ip pim rp-hash` – Displays the elected RP for the multicast group address with the mask length.

39.17 rp-candidate holdtime

Command Objective	This command configures the holdtime of the component when it is a candidate RP in the local domain. This value ranges between 0 and 255. Holdtime is the amount of time that the candidate RP advertisement is valid. This field allows advertisements to be aged out. The no form of the command sets the holdtime of the component to its default value which indicates that the local system is not a candidate RP.

Syntax	`rp-candidate holdtime <Holdtime value (0-255)>`
	
	`no rp-candidate holdtime`

Mode	PIM Component Mode
Default	0
☞	This command executes only if • PIM module is enabled globally. • PIM mode is set as sparse.
Example	`Your Product(pim-comp)# rp-candidate holdtime 25`
Related Command(s)	• `set ip pim / ip multicast` - Enables or disables the PIM globally. • `set mode` - Sets the component mode to sparse or dense. • `show ip pim rp-candidate` - Displays the RP-candidate information. • `show ip pim rp-hash` - Displays the elected RP for the multicast group address with the mask length.

39.18 rp-static rp-address

Command Objective	This command configures the address of the interface, which will be advertised as a Static-RP. Static configuration allows additional structuring of the multicast traffic by directing the multicast join/prune messages to statically configured RPs. The no form of the command disables the address of the interface, which will be advertised as a Static-RP.

Syntax	`rp-static rp-address <Group Address> <Group Mask> <IP address>`
	
	`no rp-static rp-address <Group Address> <Group Mask>`

Parameter **Description**	• `<Group Address>` - Configures the PIM Sparse multicast group address using the listed RP. • `<Group Mask>` - Configures the IP multicast group address mask that gives the group prefix for which the entry contains information about the RP. • `<IP address>` - Configures the IP address.
Mode	PIM Component Mode
☞	This command executes only if • PIM module is enabled globally. • PIM mode is set as sparse.
Example	`Your Product(pim-comp)# rp-static rp-address 224.1.0.0 255.255.0.0  20.0.0.2`
Related Command(s)	• `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally.

- `ip pim component` - Configures the PIM component in the router and enters into pim component mode.
- `ip pim componentId` - Adds the interface to the PIM component.
- `show ip pim rp-static` – Displays the RP-static information.
- `show ip pim rp-hash` – Displays the elected RP for the multicast group address with the mask length.
- `show ip pim interface` – Displays the router's PIM interfaces.

39.19 ip pim query-interval

Command Objective

This command enables PIM over an interface and configures the frequency at which PIM hello messages are transmitted on this interface. This value ranges between 0 and 65535.

The query message informs the presence of a PIM router on the interface to the neighboring PIM routers.

The no form of the command sets the default hello timer interval for this interface.

Syntax

```
ip pim query-interval <Interval (0-65535) secs>

no ip pim query-interval
```

Mode

Interface Configuration Mode (Vlan / Router)

Default

30 seconds

☞ This command executes only if PIM module is enabled globally.

Example

```
Interface Configuration Mode (Vlan)

Your Product(config)# interface vlan 3

Your Product (config-if)# ip pim query-interval 60

Interface Configuration Mode (Router)

Your Product(config)# interface gigabitethernet 0/2

Your Product(config-if)# no switchport

Your Product (config-if)# ip pim query-interval 60
```

Related Command(s)

- `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally.
- `rp-static rp-address` - Configures the address of the interface, which will be advertised as a Static-RP.

39.20 ip pim message-interval

Command Objective	This command configures the frequency at which PIM Join/ Prune messages are transmitted on the PIM interface. This value ranges between 0 and 65535. The same Join/ Prune message interval must be used on all the PIM routers in the PIM domain. If all the routers do not use the same timer interval, the performance of PIM Sparse can be adversely affected. The no form of the command resets the PIM Join/ Prune message to its default value.

Syntax	`ip pim message-interval <Interval(0-65535)>`
	
	`no ip pim message-interval`

Mode	Interface Configuration Mode (Vlan / Router)
Default	60
☞	This command executes only if PIM module is enabled globally.

Example	`Interface Configuration Mode (Vlan)`
	
	`Your Product(config)# interface vlan 3`
	
	`Your Product (config-if)# ip pim message-interval 120`
	
	`Interface Configuration Mode (Router)`
	
	`Your Product(config)# interface gigabitethernet 0/2`
	
	`Your Product(config-if)# no switchport`
	
	`Your Product (config-if)# ip pim message-interval 120`

Related Command(s)	• `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally.

39.21 ip pim bsr-candidate - value

Command Objective	This command configures the preference value for the local interface as a candidate Bootstrap Router (BSR). This preference value ranges between 0 and 255. A BSR is a dynamically elected router within a PIM domain. The router with highest priority is considered as the BSR. If the priority values are same, then the router with largest IP address is considered as the BSR. The no form of the command resets the default preference value for the local interface as a candidate bootstrap router.

Syntax	`ip pim bsr-candidate <value (0-255)>`
	
	`no ip pim bsr-candidate`

Mode	Interface Configuration Mode (Vlan / Router)
Default	0
☞	This command executes only if PIM module is enabled globally.

Example	`Interface Configuration Mode (Vlan)`
	
	`Your Product(config)# interface vlan 3`
	
	`Your Product (config-if)# ip pim bsr-candidate 1`
	
	`Interface Configuration Mode (Router)`
	
	`Your Product(config)# interface gigabitethernet 0/2`
	
	`Your Product(config-if)# no switchport`
	
	`Your Product (config-if)# ip pim bsr-candidate 1`

Related Command(s)

- `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally.
- `rp-candidate rp-address` - Sets the address of the interface, which will be advertised as a Candidate-RP.

39.22 ip pim bsr-candidate – vlan

Command Objective	This command configures the local interface as a candidate Bootstrap Router (BSR). A BSR is a dynamically elected router within a PIM domain. The router with highest priority is considered as the BSR. If the priority values are same, then the router with largest IP address is considered as the BSR. This command is a standardized implementation of the existing command; ip pim bsr-candidate - value. It operates similar to the existing command.
Syntax	`ip pim bsr-candidate <vlan-interface-no (1-4094)> [<hash-mask-length>] [priority <value(0-255)>]`
Parameter **Description**	• `<vlan-interface-no(1-4094)>` - Configures the VLAN interface number from which BSR address is derived to make BSR as a candidate. This value ranges between 1 and 4094. • `<hash-mask-length>` - Configures the IP multicast group address mask that gives the group prefix for which the entry contains information about the RP. • `priority<value(0-255)>` - Configures the priority of the candidate BSR. This value ranges between 0 and 255.
Mode	Global Configuration Mode
Default	• **hash-mask-length - 30** • **priority - 0**
☞	This command executes only if PIM module is enabled globally.
Example	`Your Product(config)# ip pim bsr-candidate 1 priority 100`

Related Command(s)

- `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally.
- `rp-candidate rp-address` - Sets the address of the interface, which will be advertised as a Candidate-RP.
- `show ip pim bsr` - Displays the BSR information.

39.23 ip pim componentId

Command Objective	This command adds the interface to the PIM component. This value ranges between 1 and 255. This command adds the current VLAN into the specified PIM component. The no form of the command removes the interface from the PIM component.

Syntax	`ip pim componentId <value(1-255)>`
	
	`no ip pim componentId <value(1-255)>`

Mode	Interface Configuration Mode (Vlan / Router)
Default	1
☞	This command executes only if • PIM module is enabled globally. • PIM component is configured in the router.
Example	**Interface Configuration Mode (Vlan)** **Your Product(config)# interface vlan 3** **Your Product (config-if)# ip pim componentId 1** **Interface Configuration Mode (Router)** **Your Product(config)# interface gigabitethernet 0/2** **Your Product(config-if)# no switchport** **Your Product (config-if)# ip pim componentId 1**

Related Command(s)

- `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally.
- `ip pim component` - Configures the PIM component in the router.
- `rp-candidate rp-address` - Sets the address of the interface, which will be advertised as a Candidate-RP.
- `rp-static rp-address` - Sets the address of the interface, which will be advertised as a Static-RP.
- `show ip pim interface` - Displays the routers PIM interfaces.
- `set ip pim graft-retry interval` - Configures the time before which graft is retransmitted upon no receipt of Graft ACK.
- `show ip pim component` - Displays the component information.
- `set ipv6 pim graft-retry interval` - Configures the time before which graft is retransmitted upon no receipt of Graft ACK.

39.24 ip pim dr-priority

Command Objective	This command configures the designated router priority value configured for the router interface. This value ranges between 1 and 4294967295. The no form of the command sets the default designated router priority value for the router interface. The DR sets up multicast route entries and sends corresponding Join/Prune and Register messages on behalf of directly-connected receivers and sources, respectively.

Syntax	`ip pim dr-priority <priority>`
	
	`no ip pim dr-priority`

Mode	Interface Configuration Mode (Vlan / Router)
Default	1
☞	This command executes only if PIM module is enabled globally.

Example	`Interface Configuration Mode (Vlan)`
	
	`Your Product(config)# interface vlan 3`
	
	`Your Product (config-if)# ip pim dr-priority 100`
	
	`Interface Configuration Mode (Router)`
	
	`Your Product(config)# interface gigabitethernet 0/2`
	
	`Your Product(config-if)# no switchport`
	
	`Your Product (config-if)# ip pim dr-priority 100`

Related Command(s)	• `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally. • `show ip pim interface` - Displays the routers PIM interfaces.

39.25 ip pim override-interval

Command Objective	This command configures the override interval configured for router interface. This value ranges between 0 and 65535. Override interval is the random amount of time delayed for sending override messages to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The no form of the command sets the default override interval for router interface.

Syntax	`ip pim override-interval <interval(0-65535)>`
	
	`no ip pim override-interval`

Mode	Interface Configuration Mode (Vlan / Router)
Default	0
☞	This command executes only if PIM module is enabled globally.
Example	**Interface Configuration Mode (Vlan)** **Your Product(config)# interface vlan 3** **Your Product (config-if)# ip pim override-interval 100** **Interface Configuration Mode (Router)** **Your Product(config)# interface gigabitethernet 0/2** **Your Product(config-if)# no switchport** **Your Product (config-if)# ip pim override-interval 100**
Related Command(s)	• `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally. • `show ip pim interface` - Displays the routers PIM interfaces.

39.26 ip pim lan-delay

Command Objective	This command configures the LanDelay configured for the router interface. This value ranges between 0 and 65535. The LAN Delay inserted by a router in the LAN Prune Delay option expresses the expected message propagation delay on the interface. It is used by upstream routers to find out the delayed time interval for a Join override message before pruning an interface. The no form of the command sets the default LanDelay for the router per interface.

Syntax	`ip pim lan-delay <value(0-65535)>`
	
	`no ip pim lan-delay`

Mode	Interface Configuration Mode (Vlan / Router)
Default	0
☞	This command executes only if PIM module is enabled globally.
Example	**Interface Configuration Mode (Vlan)** **Your Product(config)# interface vlan 3** **Your Product (config-if)# ip pim lan-delay 120** **Interface Configuration Mode (Router)** **Your Product(config)# interface gigabitethernet 0/2** **Your Product(config-if)# no switchport** **Your Product (config-if)# ip pim lan-delay 120**
Related Command(s)	• `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally. • `set ip pim lan-prune-delay` - Enables / disables the LanPruneDelay.

39.27 set ip pim lan-prune-delay

Command Objective	This command enables / disables the LanPruneDelay bit configured for the router interface to advertise the Lan delay. The command specifies whether to use LAN prune delay or not.
Syntax	`set ip pim lan-prune-delay { enable | disable }`
Parameter Description	• `enable` - Enables LAN-prune-delay. • `disable` - Disables LAN-prune-delay.
Mode	Interface Configuration Mode (Vlan / Router)
Default	disable
☞	This command executes only if PIM module is enabled globally.
Example	**Interface Configuration Mode (Vlan)** **Your Product(config)# interface vlan 3** **Your Product (config-if)# set ip pim lan-prune-delay enable** **Interface Configuration Mode (Router)** **Your Product(config)# interface gigabitethernet 0/2** **Your Product(config-if)# no switchport** **Your Product (config-if)# set ip pim lan-prune-delay enable**
Related Command(s)	• `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally. • `ip pim lan-delay` - Configures the LanDelay configured for the router interface. • `show ip pim interface` - Displays the routers PIM interfaces.

39.28 set ip pim graft-retry interval

Command Objective	This command configures the time before which graft is retransmitted upon no receipt of Graft ACK. This value ranges between 1 and 10. The no form of the command sets the graft retry interval to its default value.

Syntax	`set ip pim graft-retry interval <value(1-10)>`
	
	`no ip pim graft-retry interval`

Mode	Interface Configuration Mode (Vlan / Router)
Default	3 seconds
☞	This command executes only if PIM module is enabled globally. To configure the graft-retry interval, the PIM component that the interface is mapped to should be in dense mode.
Example	**Interface Configuration Mode (Vlan)** **Your Product(config)# interface vlan 3** **Your Product (config-if)# set ip pim graft-retry interval 4** **Interface Configuration Mode (Router)** **Your Product(config)# interface gigabitethernet 0/2** **Your Product(config-if)# no switchport** **Your Product (config-if)# set ip pim graft-retry interval 4**
Related Command(s)	• `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally. • `set mode` - Sets the component mode to sparse or dense. • `ip pim componentId` - Adds the interface to the PIM component. • `show ip pim interface` - Displays the routers PIM interfaces.

39.29 no ip pim interface

Command Objective	This command deletes an interface at PIM level. This command is used to destroy the interface at PIM.
Syntax	`no ip pim interface`
Mode	Interface Configuration Mode (Vlan / Router)
☞	This command executes only if PIM module is enabled globally.

Example	`Interface Configuration Mode (Vlan)`
	`Your Product(config)# interface vlan 3`
	`Your Product (config-if)# no ip pim interface`
	`Interface Configuration Mode (Router)`
	`Your Product(config)# interface gigabitethernet 0/2`
	`Your Product(config-if)# no switchport`
	`Your Product (config-if)# no ip pim interface`

Related Command(s)	• `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally. • `show ip pim interface` - Displays the routers PIM interfaces.

39.30 debug ip pim

Command Objective

This command enables the tracing of the PIM module as per the configured debug levels. The trace statements are generated for the configured trace levels.

This command allows combination of debug levels to be configured (that is, more than one level of trace can be enabled or disabled). The debug levels are configured one after the other and not in single execution of the command.

A Four byte integer value is specified for enabling the level of debugging. Each bit in the four byte integer variable represents a level of debugging. The combinations of levels are also allowed. The user has to enter the corresponding integer value for the bit set.

Syntax

```
debug ip pim
{[nbr][grp][jp][ast][bsr][io][pmbr][mrt][mdh][mgmt][srm
][red] | [all]}

no debug ip pim
{[nbr][grp][jp][ast][bsr][io][pmbr][mrt][mdh][mgmt][srm
][red] | [all]}
```

Parameter Description

- `nbr` - Sets the module as PIM Neighbor Discovery module, for which the tracing is to be done as per the configured debug levels.
- `grp` - Generates debug statements for Group Membership traces.
- `jp` - Generates debug statements for Join or Prune traces.
- `ast` - Generates debug statements for Assert state traces.
- `bsr` - Generates debug statements for Bootstrap/RP traces.
- `io` - Generates debug statements for Input Output traces.
- `pmbr` - Generates debug statements for Interoperability traces.
- `mrt` - Generates debug statements for Multicast Route Table Update traces.
- `mdh` - Generates debug statements for Multicast Data Handling traces.
- `mgmt` - Generates debug statements for management traces.

	• **srm** - Generates debug statements for state refresh messages. • **red** - Sets the module as PIM redundancy module, for which the tracing is to be done as per the configured debug levels. • **all** - Generates debug statements for all kinds of traces.
Mode	Privileged EXEC Mode
☞	This command executes only if PIM module is enabled globally.
Example	`Your Product # debug ip pim all`
Related Command(s)	• **set ip pim / ip multicast** - Enables / disables PIM feature in the switch globally. • **show ip pim interface** - Displays the routers PIM interfaces.

39.31 show ip pim interface

Command Objective

This command displays the router's PIM interfaces. The information contains the list of Interface addresses, the mode of the interface, Designated Router on that interface, Hello Interval, Join/Prune Interval of the interface, offer limit and offer interval.

Syntax

```
show ip pim interface [{ Vlan <vlan-id/vfi-id> |
<interface-type> <interface-id> [df] | <IP-interface-
type> <IP-interface-number> | detail }]
```

Parameter

Description

- `Vlan <vlan-id/vfi-id>` - Displays PIM configurations 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.
- `<interface-type>` - Displays PIM configurations 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>** - Displays PIM configurations 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 is provided, for interface type i-lan. For example: 1 represents i-lan.

- **<IP-interface-type>** - Display PIM configuration for the specified L3 Psuedo wire interface in the system.

- **<IP-interface-number>** - Display PIM configuration 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.

- **detail** - Displays the detailed PIM information fro the interface.

Mode	Privileged EXEC Mode
☞	This command executes only if PIM module is enabled globally.

Example

```
Your Product(config)# show ip pim interface
Address IfName/IfId Ver/Mode Nbr  Qry    DR-Address DR-Prio
                             Count Interval
10.0.0.1  vlan1/160 2/Sparse   0   45    10.0.0.1     5
20.0.0.1  vlan2/33  2/Sparse   0   30    20.0.0.1     1
30.0.0.1  vlan3/34  2/Sparse   0   60    30.0.0.1     1
Your Product# show ip pim interface vlan 1
Address IfName/IfId Ver/Mode Nbr Qry     DR-Address DR- Prio
                               Count Interval
10.0.0.1  vlan1/160  2/Sparse  0  45      10.0.0.1    5
Your Product# show ip pim interface detail
vlan1 73 is up
  Internet Address is 11.0.0.1
  Muticast Switching : Enabled
  PIM : Enabled
  PIMv6 : Enabled
    PIM version : 2, mode: Sparse
    PIM DR : 11.0.0.1
    PIM DR Priority : 1
    PIM Neighbour Count : 0
    PIM Hello/Query Interval : 30
    PIM Message Interval : 60
    PIM Override Interval : 0
    PIM Lan Delay : 0
    PIM Lan-Prune-Delay : Disabled
    PIM Component Id : 1
    PIM domain border : disabled
    PIM RPF Status : Disabled
    Offer Interval : 100, Offer Limit : 4
```

Related Command(s)

- `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally.
- `ip pim componentId` – Adds the interface to the PIM component.
- `ip pim component` - Configures the PIM component in the router.
- `ip pim version` - Configures version number of the PIM protocol in the switch.
- `ip pim query-interval` – Sets the frequency at which PIM hello messages are transmitted on this interface.
- `ip pim message-interval` – Sets the frequency at which PIM Join/Prune messages are transmitted on this PIM interface.
- `ip pim bsr-candidate - value` – Sets the preference value for the local interface as a candidate bootstrap router.
- `ip pim dr-priority` – Sets the designated router priority value configured for the router interface.
- `ip pim override-interval` – Sets the override interval configured for router interface.
- `ip pim lan-delay` – Sets the LanDelay configured for the router interface.
- `set ip pim lan-prune-delay` – Sets the LanPruneDelay bit configured for the router interface to advertise the lan delay.
- `no ip pim interface` – Deletes an interface at PIM level.
- `debug ip pim` – Enables PIM trace.

39.32 show ip pim neighbor

Command Objective

This command displays the router's PIM neighbors' information. The information contains the Neighbor Address, the interface used to reach the PIM Neighbor, the Up time (the time since this neighbor became the neighbor of the local router), Expiry Time (the min. time remaining before this PIM neighbor will be aged out), LAN delay and Override interval.

Syntax

```
show ip pim neighbor [{ Vlan <vlan-id/vfi-id> |
<interface-type> <interface-id> | <IP-interface-type>
<IPinterface-number>}]
```

Parameter

Description

- `Vlan <vlan-id/vfi-id>` - Displays PIM neighbor configurations 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.

- **<interface-type>** - Displays the router's PIM neighbors' information 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>** - Displays PIM configurations 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 is provided, for interface type i-lan. For example: 1 represents i-lan.
- **<IP-interface-type> -** Display PIM neighbor configuration for the specified L3 Psuedo wire interface in the system.
- **<IP-interface-number> -** Display PIM neighbor configuration 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	Privileged EXEC Mode
☞	This command executes only if PIM module is enabled globally.

Example

```
Your Product(config)# show ip pim neighbor vlan 1

Neighbour    IfName/Idx Uptime/Expiry Ver DRPri    CompId    Override
LanDelay

Address                                  /Mode          Interval

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

12.0.0.2     vlan1/33   00:00:45/275   v2  1       1    0       0
```

Related Command(s)

- **set ip pim / ip multicast** - Enables / disables PIM feature in the switch globally.
- **ip pim componentId** – Adds the interface to the PIM component.
- **ip pim component** - Configures the PIM component in the router.
- **ip pim query-interval** – Sets the frequency at which PIM hello messages are transmitted on this interface.
- **ip pim message-interval** – Sets the frequency at which PIM Join/Prune messages are transmitted on this PIM interface.
- **ip pim bsr-candidate - value** – Sets the preference value for the local interface as a candidate bootstrap router.

39.33 show ip pim rp-candidate

Command Objective	This command displays the candidate RP information. The information contains the Group addresses, the Group Mask and the RP address that indicates the IP address of the Rendezvous Point (RP) for the listed PIM Sparse group.
Syntax	`show ip pim rp-candidate [ComponentId <1-255>]`
Parameter Description	• `ComponentId <1-255>` - Displays the specified Component ID for which the candidate RP information is to be displayed. The value ranges between 0 and 255.
Mode	Privileged EXEC Mode
☞	This command executes only if PIM module is enabled globally.

Example	`Your Product# show ip pim rp-candidate 2`
	`CompId GroupAddress Group Mask RPAddress/Priority`
	`2 224.1.0.0 255.255.0.0 20.0.0.1/192`

Related Command(s)

- `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally.
- `ip pim component` – Configures the PIM component in the router.
- `ip pim componentId` - Adds the interface to the PIM component.
- `ip pim bsr-candidate – value / ip pim bsr-candidate – vlan` - Configures the local interface as a candidate Bootstrap Router.
- `rp-candidate rp-address` – Enables the address of the interface, which will be advertised as a Candidate-RP.
- `rp-candidate holdtime` – Sets the holdtime of the component when it is a candidate RP in the local domain.
- `rp-static rp-address` – Sets the address of the interface, which will be advertised as a Static-RP.
- `show ip pim rp-hash` - Displays the elected RP for the multicast group address with the mask length.

39.34 show ip pim rp-set

Command Objective	This command displays the RP-set information. This information includes details of the Group Prefix, RP address, Hold time and Expiry Time.
Syntax	`show ip pim rp-set [rp-address]`
Parameter Description	• `rp-address` - Displays the IP address of the Rendezvous Point (RP) for the listed PIM Sparse group.
Mode	Privileged EXEC Mode
☞	This command executes only if PIM module is enabled globally.

Example

```
Your Product# show ip pim rp-set
PIM Group-to-RP mappings
---------------------------
Group Address: 224.1.0.0  Group Mask: 255.255.0.0
    RP: 20.0.0.1
    Component-Id: 2
    Hold Time: 120, Expiry Time: 00:01:43
```

Related Command(s)

- `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally.
- `ip pim component` – Configures the PIM component in the router.
- `ip pim componentId` - Adds the interface to the PIM component.
- `ip pim bsr-candidate – value / ip pim bsr-candidate – vlan` - Configures the local interface as a candidate Bootstrap Router.
- `rp-candidate rp-address` – Enables the address of the interface, which will be advertised as a Candidate-RP.
- `set ip pim static-rp` – Enables or disables the Static RP configuration Status.
- `rp-candidate holdtime` - Sets the holdtime of the component when it is a candidate RP in the local domain.
- `rp-static rp-address` – Sets the address of the interface, which will be advertised as a Static-RP.
- `show ip pim rp-hash` - Displays the elected RP for the multicast group address with the mask length.

39.35 show ip pim bsr

Command Objective	This command displays the BSR information. The component ID value ranges between 1 and 255.
Syntax	`show ip pim bsr [Component-Id (1-255)]`
Mode	Privileged EXEC Mode
☞	This command executes only if PIM module is enabled globally.

Example	**`Your Product# show ip pim bsr 1`**
	`PIMv2 Bootstrap Configuration For Component 1`
	`------------------------------------------------`
	`This system is the Bootstrap Router (BSR)`
	`BSR Address: 10.0.0.1`
	`BSR Priority: 6, Hash Mask Length: 30`

Related Command(s)	• **`ip pim component`** – Configures the PIM component in the router. • **`ip pim componentId`** - Adds the interface to the PIM component. • **`set ip pim/ ip multicast`** - Enables / disables PIM feature in the switch globally. • **`ip pim bsr-candidate – value`** – Sets the preference value for the local interface as a candidate bootstrap router. • **`ip pim bsr-candidate – VLAN`** – Sets the local interface as a candidate bootstrap router.

39.36 show ip pim rp-static

Command Objective	This command displays the static RP information. The component ID value ranges between 1 and 255.
Syntax	`show ip pim rp-static [ComponentId <1-255>]`
Parameter Description	• `ComponentId <1-255>` - Displays the Specified the Component ID for which the static RP information is to be displayed. The value ranges between 1 and 255.
Mode	Privileged EXEC Mode
☞	This command executes only if PIM module is enabled globally.

Example

```
Your Product# show ip pim rp-static 2

Static-RP Enabled

  CompId   GroupAddress   Group Mask        RPAddress

    2      225.1.0.0      255.255.0.0       20.0.0.1
```

Related Command(s)

- `set ip pim / ip multicast` - Enables / disables PIM feature in the switch globally.
- `ip pim component` – Configures the PIM component in the router.
- `ip pim componentId` - Adds the interface to the PIM component.
- `rp-candidate holdtime` - Sets the holdtime of the component when it is a candidate RP in the local domain.
- `rp-static rp-address` – Sets the address of the interface, which will be advertised as a Static-RP.
- `shutdown – physical/VLAN/port-channel/tunnel interface` – Disables a physical interface / VLAN interface / port-channel interface / tunnel interface / OOB interface.

- `ip address` - Configures IP address on the interface.
- `set ip pim static-rp` – Enables or disables the Static RP configuration Status.
- `rp-static rp-address` - Sets the address of the interface, which will be advertised as a Static-RP.
- `show ip pim rp-hash` - Displays the elected RP for the multicast group address with the mask length.

39.37 show ip pim component

Command Objective	This command displays the component information. The component ID value ranges between 1 and 255.
Syntax	`show ip pim component [ComponentId <1-255>]`
Mode	Privileged EXEC Mode
☞	This command executes only if PIM module is enabled globally.

Example	**`Your Product# show ip pim component 1`**
	`PIM Component Information`
	`----------`
	`Component-Id: 1`
	`PIM Mode: sparse, PIM Version: 2`
	`Elected BSR: 10.0.0.1`
	`Candidate RP Holdtime: 0`

Related Command(s)	• **`set ip pim / ip multicast`** - Enables / disables PIM feature in the switch globally. • **`ip pim component`** – Configures the PIM component in the router. • **`ip pim componentId`** - Adds the interface to the PIM component. • **`ip pim version`** - Configures version number of the PIM protocol in the switch.

39.38 show ip pim thresholds

Command Objective	This command displays threshold configured for SPT, RP thresholds, and rate limit values for both SM (Sparse mode).
Syntax	`show ip pim thresholds`
Mode	Privileged EXEC Mode
☞	This command executes only if PIM module is enabled globally.

Example	**`Your Product# show ip pim thresholds`**
	`PIM SPT Threshold Information`
	`Group Threshold: 0`
	`Source Threshold: 0`
	`Switching Period: 0`
	`PIM SPT-RP Threshold Information`
	`Register Threshold: 0`

Related Command(s)	• **`set ip pim / ip multicast`** - Enables / disables PIM feature in the switch globally. • **`set ip pim threshold`** – Specifies the SPT group or source threshold when exceeded, switching to shortest path tree is initiated. • **`set ip pim spt-switchperiod`** – Specifies the period (in seconds) over which the data rate is to be monitored for switching to shortest path tree. • **`set ip pim rp-threshold`** – Specifies the threshold at which the RP initiates switching to source specific shortest path tree. • **`set ip pim rp-switchperiod`** – Specifies the period (in seconds) over which RP monitors register packets for switching to the source specific shortest path tree.

- **`set ip pim regstop-ratelimit-period`** – Specifies the period over which RP monitors number of register packets after sending the register stop message.
- **`set ip pim pmbr`** – Enables or disables the PMBR (PIM Multicast Border Router) Status.
- **`ip pim dr-priority`** – Sets the designated router priority value configured for the router interface.

39.39 show ip pim mroute

Command Objective

This command displays the PIM multicast information.mroutes are multicast routing cache entries created by a user level mrouting daemon.

Syntax

```
show ip pim mroute [ {proxy | {compid(1-255) | group-address | source-address } summary }]
```

Parameter Description

- `proxy` - Displays RPF vector information.
- `Compid(1-255)` - Displays the component ID. The value ranges between 1 and 255.
- `group-address` - Displays the PIM multicast group address using the listed RP.
- `source-address` - Displays the network address which identifies the sources for which this entry contains multicast routing information.
- `summary` - Displays the summary of PIM mroute information.

Mode

Privileged EXEC Mode

This command executes only if PIM module is enabled globally.

Example

```
Your Product# show ip pim mroute
IP Multicast Routing Table
--------------------------
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
IIF State P: Pruned F: Forwarding A: Graft Ack Pending
Timers: Uptime/Expires
Interface State: Interface, State/Mode
PIM Multicast Routing Table For Component 1
```

```
(12.0.0.10,227.1.1.1) ,00:00:03/05:43:11 Incoming
Interface : vlan1 ,RPF nbr : NULL ,Route Flags : ---

  IIF State : P ,SRM Generation  : Enabled

  Source Active Timer Value 210

  Source Active Remaining Time : 05:43:11

  State Refresh Remaining Time : 00:00:00

  Prune Limit Remaing Time : 00:00:00

Outgoing Interface List : NULL
```

Your Product# show ip pim mroute 1 summary

```
IP Multicast Routing Table

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

Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit

Timers : Uptime/Expires

Interface State : Interface, State/Mode

PIM Multicast Routing Table For Component 1

(*, 224,1,0.0) , 00:04:35/--- , RP : 12.0.0.1

Incoming Interface : vlan1, RPF nbr : NULL, Route
Flags : WR

Outgoing Interface List:

 vlan2, Forwarding/Sparse, 00:04:35/---
(12.0.0.30,224.1.0.0) , 00:00:04/00:03:26

Incoming Interface : vlan1, RPF nbr : NULL, Route
Flages : S
```

```
Outgoing InterfaceList :

vlan2, Forwarding/Sparse , 00:00:04/---

Your Product# show ip pim mroute

IP Multicast Routing Table

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

Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit

IIF State P: Pruned F: Forwarding A: Graft Ack Pending

Timers: Uptime/Expires
```

Related Command(s)

- **ip pim component** – Configures the PIM component in the router.
- **set ip pim / ip multicast** - Enables / disables PIM feature in the switch globally.
- **ip pim bsr-candidate - value** - Sets the preference value for the local interface as a candidate bootstrap router.

39.40 show ip pim redundancy state

Command Objective	This command displays the status of PIM HA feature (enabled/disabled), status of active and standby PIM instance and status of dynamic bulk update.
Syntax	`show ip pim redundancy state`
Mode	Privileged EXEC Mode

Example	`Your Product# show ip pim redundancy state`
	`Hot-standby feature is Enabled.`
	`Node State: Active,Standby Down .`
	`Dynamic Bulk Updates not started`

39.41 show ip pim redundancy shadow-table

Command Objective	This command displays the shadow-table information for PIMv4 Route entries.
Syntax	`show ip pim redundancy shadow-table`
Mode	Privileged EXEC Mode

Example

```
Your Product#  show ip pim redundancy shadow-table
Forwarding Plane Shadow Table :
------------------------------
(S, G)
Incoming interface:( Alias / IfIndex)
CPU Port Flag     :CPU Port Added / CPU Port Not Added
Route Mode        : Sparse / Dense
Route Status      : UnProcessed/Refreshed /New
Outgoing InterfaceList :( Alias / IfIndex)
(80.0.0.2, 224.6.6.6)
Incoming interface:(vlan4 / 38)
CPU Port Flag     :CPU Port Not Added
Route Mode        :Dense
Route Status      :New
Outgoing InterfaceList :
        (vlan2 / 36), (vlan14 / 34),
(80.0.0.3, 224.6.6.6)
```

```
Incoming interface:(vlan4 / 38)

CPU Port Flag     :CPU Port Not Added

Route Mode        :Dense

Route Status      :New

Outgoing InterfaceList :

         (vlan2 / 36), (vlan14 / 34),

 Number of Entries : 2
```

39.42 ip pim bsr-border

Command Objective	This command sets a PIM domain BSR (Bootstrap router) message border for an interface which stops the BSR message forwarding over the specified interface. The no form of the command resets the PIM domain BSR message border.

Syntax	`ip pim bsr-border`
	
	`no ip pim bsr-border`

Mode	Interface Configuration Mode (VLAN/ Router)
☞	This command executes only if PIM module is enabled globally.
Example	`Your Product(config-if)# ip pim bsr-border`
Related Command(s)	• `set ip pim` - Enables or disables the PIM globally.

39.43 set ip pim rpf vector

Command Objective	This command enables or disables the PIM RPF Vector TLV feature.
Syntax	`set ip pim rpf vector { enable | disable }`
Parameter Description	• `enable` - Enables RPF vector. • `disable` - Disables RPF vector.
Mode	Global Configuration Mode
☞	This command executes only if PIM module is enabled.
Example	`Your Product(config)# set ip pim rpf vector enable`
Related Command(s)	• `set ip pim/ ip multicast` - Enables / disables PIM feature in the switch globally.

39.44 show ip pim rp-hash

Command Objective	This command displays the elected RP for the multicast group address with the mask length.
Syntax	`show ip pim rp-hash [<multicast_Group_address> <Group_mask>]`
Parameter Description	• `<multicast_Group_address>` - Specifies the IP multicast group address for which this entry contains multicast routing information. • `<Group_Mask>` - Specifies the IP multicast group address mask that, gives the group prefix for which this entry contains information about the RP.
Mode	Privileged EXEC Mode

Example	`Your Product (config)# show ip pim rp-hash`
	`Component 1`
	`----------`
	`Group Address/Network Mask: 224.1.0.0/255.255.0.0`
	`RP Address: 20.0.0.0`
	`Priority: 192, Hold Time: 0`

Related Command(s)	• `set ip pim` – Enables/ disables PIM globally. • `rp-candidate rp-address` – Sets the address of the interface, which will be advertised as a Candidate-RP. • `ip pim bsr-candidate` - Sets the Preference value for the local PIM interface as a candidate bootstrap router. • `rp-candidate holdtime` - Configures the holdtime of the component when it is a candidate RP in the local domain.

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