IP Configuration

This chapter contains the following sections:

IPv4 Management and Interfaces

IP interface addresses can be configured manually by the user, or automatically configured by a DHCP server. This section provides information for defining the device IP addresses, either manually or by making the device a DHCP client. This section covers the IPv4 management and interfaces.

IPv4 Interface

IPv4 interface addresses can be configured manually by the user, or automatically configured by a DHCP server. This section provides information for defining the device IPv4 addresses, either manually or by making the device a DHCP client. The IPv4 Interface page is used to configure IP addresses for device management. This IP address can be configured on a port, a LAG, VLAN, loopback interface or out-of-band interface. You can configure multiple IP addresses (interfaces) on the device. It then supports traffic routing between these various interfaces and also to remote networks. By default and typically, the routing functionality is performed by the hardware. If hardware resources are exhausted or there's a routing table overflow in the hardware, IP routing is performed by the software.

Note The device software consumes one VLAN ID (VID) for every IP address configured on a port or LAG. The device takes the first VID that isn't used starting from 4094.

To configure the IPv4 addresses, follow these steps:

Step 1 Click **IP Configuration** >**IPv4 Management and Interfaces** > **IPv4 Interface.**

Enter the following fields:

- IPv4 Routing—Check the Enable box to enable IPv4 routing (enabled by default).

Step 2 Click **Apply**. The parameter is saved to the Running Configuration file.

The following fields are displayed in the IPv4 Interface Table:

- Interface—Interface for which the IP address is defined. This can also be the out-of-band port.
- IP Address Type—The available options are:
  - DHCP—Received from DHCP server
  - Static—Entered manually. Static interfaces are non-DHCP interfaces that created by the user.
  - Default—The default address that exists on the device by default, before any configurations have been made.
- IP Address—Configured IP address for the interface.
- Mask—Configured IP address mask.
- Status—Results of the IP address duplication check.
  - Tentative—There's no final result for the IP address duplication check.
  - Valid—The IP address collision check was completed, and no IP address collision was detected.
  - Valid-Duplicated—The IP address duplication check was completed, and a duplicate IP address was detected.
  - Duplicated—A duplicated IP address was detected for the default IP address.
  - Delayed—The assignment of the IP address is delayed for 60 second if DHCP Client is enabled on startup in order to give time to discover DHCP address.
  - Not Received—Relevant for DHCP Address When a DCHP Client starts a discovery process, it assigns a dummy IP address 0.0.0.0 before the real address is obtained. This dummy address has the status of "Not Received".

Step 3 Click **Add.**

Step 4 Select the Interface: Select the port, LAG, VLAN or loopback as the interface associated with this IP configuration, and select an interface from the list. select an interface from the associated list.

Step 5 Select the IP Address Type: Select one of the following options:

- Dynamic IP Address—Receive the IP address from a DHCP server.
- Static IP Address—Enter the IP address, and enter the Mask field:
  - Network Mask—IP mask for this address
  - Prefix Length—Length of the IPv4 prefix

Step 6 Click **Apply**. The IPv4 address settings are written to the Running Configuration file.

Caution When the system is in one of the stacking modes with a Active Backup present, Cisco recommends configuring the IP address as a static address to prevent disconnecting from the network during a stacking active unit switchover. This is because when the stack standby unit takes control of the stack, when using DHCP, it might receive a different IP address than the one that was received by the stack's original active unit.

IPv4 Static Routes

This page enables configuring and viewing IPv4 static routes on the device. When routing traffic, the next hop is decided on according to the longest prefix match (LPM algorithm). A destination IPv4 address may match multiple routes in the IPv4 Static Route Table. The device uses the matched route with the highest subnet mask, that is, the longest prefix match. If more than one default gateway is defined with the same metric value, the lowest IPv4 address from among all the configured default gateways is used.

To define an IP static route, follow these steps:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **IPv4 Static Routes**.

The IPv4 Static Routes Table is displayed. The following fields are displayed for each entry:

- Destination IP Prefix-Destination IP address prefix.
- Prefix Length- IP route prefix for the destination IP.
- Route Type-Whether the route is a reject or remote route.
- Next Hop Router IP Address-The next hop IP address or IP alias on the route.
- Metric-Cost of this hop (a lower value is preferred).
- Outgoing Interface-Outgoing interface for this route.

Step 2 Click **Add.**

Step 3 Enter values for the following fields:

- Destination IP Prefix-Enter the destination IP address prefix.
- Mask-Select and enter:
  - Network Mask-IP route prefix for the destination IP, in the format of a mask (number of bits in of route network address)
  - Prefix Length-IP route prefix for the destination IP in IP address format
- Route Type-Select the route type.
  - Reject-Rejects the route and stops routing to the destination network via all gateways This ensures that if a frame arrives with the destination IP of this route, it’s dropped. Selecting this value disables the following controls: Next Hop IP Address, Metric, and IP SLA Track.
  - Remote-Indicates that the route is a remote path
- Next Hop Router IP Address-Enter the next hop IP address or IP alias on the route.

  Note You can’t configure a static route through a directly connected IP subnet where the device gets its IP address from a DHCP server.

- Metric select one of the following:
  - Use Default - select this to use the default metric.
  - User Defined - Enter the administrative distance to the next hop. The range is 1–255.

Step 4 Click **Apply**. The IP Static route is saved to the Running Configuration file.

IPv4 Forwarding Table

To view the IPv4 Forwarding Table, follow these steps:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** >**IPv4 Forwarding Table**.

The IPv4 Forwarding Table is displayed. The following fields are displayed for each entry:

- Destination IP Prefix—Destination IP address prefix.
- Prefix Length— IP route prefix for the length of the destination IP.
- Route Type—Whether the route is a local, reject or remote route.
- Next Hop Router IP Address—The next hop IP address.
- Route Owner—This can be one of the following options:
  - Default—Route was configured by default system configuration.
  - Static—Route was manually created.
  - Dynamic—Route was created by an IP routing protocol.
  - DHCP—Route was received from a DHCP server.
  - Directly Connected—Route is a subnet to which the device is connected.
- Metric—Cost of this hop (a lower value is preferred).
- Administrative Distance—The administrative distance to the next hop (a lower value is preferred). This isn't relevant for static routes.
- Outgoing Interface—Outgoing interface for this route.

Step 2 Click the **Refresh** icon to refresh the data.

RIPv2

This section describes the Routing Information Protocol (RIP) version 2 feature.

Routing Information Protocol (RIP) is an implementation of a distance-vector protocol for local and wide-area networks. It classifies routers as either active or passive (silent). Active routers advertise their routes to others; passive routers listen and update their routes based on advertisements, but do not advertise. Typically, routers run RIP in active mode, while hosts use passive mode.

The default gateway is a static route and it is advertised by RIP in the same way as all other static routers, if it is enabled by configuration.

When IP Routing is enabled, RIP works fully. When IP Routing is disabled, RIP works in the passive mode, meaning that it only learns routes from the received RIP messages and does not send them.

Note To enable IP Routing, go to the IPv4 Interface, on page 1 page.

The device supports RIP version 2, which is based on the following standards:

- RFC2453 RIP Version 2, November 1998
- RFC2082 RIP-2 MD5 Authentication, January 1997
- RFC1724 RIP Version 2 MIB Extension

Received RIPv1 packets are dropped.

Enabling RIP

- RIP must be enabled globally and per interface.
- RIP can only be configured if it is enabled.
- Disabling RIP globally deletes the RIP configuration on the system.
- Disabling RIP on an interface deletes the RIP configuration on the specified interface.
- If IP Routing is disabled, RIP messages are not sent, although when RIP messages are received, they are used to update the routing table information.

Note RIP can only be defined on manually-configured IP interfaces, meaning that RIP cannot be defined on an interface whose IP address was received from a DHCP server or whose IP address is the default IP address.

RIPv2 Properties

Note This feature is only supported on 550 family of devices.

To enable/disable RIP on the device.

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces**> **RIPv2** > **RIPv2 Properties**.

Step 2 Select the following options as required:

- RIP—The following options are available:
  - Enable—Enable RIP.
  - Disable—Disable RIP. Disabling RIP deletes the RIP configuration on the system.
  - Shutdown—Set the RIP global state to shutdown.

- RIP Advertisement—Select to enable sending routing updates on all RIP IP interfaces.
- Default Route Advertisement—Select to enable sending the default route to the RIP domain. This route serves as the default router.
- Default Metric—Enter the value of the default metric.

Step 3 Redistribute Static Route—Select to enable this feature.

Step 4 If Redistribute Static Route is enabled, select an option for the Redistribute Static Metric field. The following options are available:

- Default Metric—Causes RIP to use the default metric value for the propagated static route configuration..
- Transparent—Causes RIP to use the routing table metric as the RIP metric for the propagated static route configuration. This results in the following behavior:
  - If the metric value of a static route is equal to or less than 15, this value is used in the RIP protocol when advertising this static route.
  - If the metric value of a static route is greater than 15, the static route isn't advertised to other routers using RIP.
- User-Defined Metric—Enter the value of the metric.

Step 5 Redistribute Connected Route—Select to enable this feature (described in Redistributing Static Route Configuration.

Step 6 If Redistribute Connected Route is enabled, select an option for the Redistribute Connected Metric field. The following options are available:

- Default Metric—Causes RIP to use the default metric value for the propagated static route configuration.
- Transparent—Causes RIP to use the routing table metric as the RIP metric for the propagated static route configuration. This results in the following behavior:
  - If the metric value of a static route is equal to or less than 15, this value is used in the RIP protocol when advertising this static route.
  - If the metric value of a static route is greater than 15, the static route isn't advertised to other routers using RIP.
- User-Defined Metric—Enter the value of the metric.

Step 7 Click **Apply**. The settings are written to the Running Configuration file.

RIPv2 Settings

To configure RIP on an IP interface:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **RIPv2** > **RIPv2 Settings**.

Step 2 RIP parameters are displayed per IP interface. To add a new IP interface, click **Add** and enter the following fields:

- IP Address—Select an IP interface defined on the Layer 2 interface.
- Shutdown—Keep RIP configuration on the interface, but set the interface to inactive.

- Passive—Specifies whether sending RIP route update messages is allowed on the specified IP interface. If this field isn't enabled, RIP updates aren't sent (passive).
- Offset—Specifies the metric number of the specified IP interface. This reflects the additional cost of using this interface, based on the speed of the interface.
- Default Route Advertisement—This option is defined globally in the RIPv2 Properties, on page 5 page. You can use the global definition or define this field for the specific interface. The following options are available:
  - Global—Use the global settings defined in the RIPv2 Properties. Screen
  - Disable—On this RIP interface, don't advertise the default route.
  - Enable—Advertise the default route on this RIP interface.
- Default Route Advertisement Metric—Enter the metric for the default route for this interface.
- Authentication Mode—RIP authentication state (enable/disable) on a specified IP interface. The following options are available:
  - None—There's no authentication performed.
  - Text—The key password entered below is used for authentication.
  - MD5—The MD5 digest of the key chain selected below is used for authentication.
- Key Password—If Text was selected as the authentication type, enter the password to be used.
- Key Chain—If MD5 was selected as the authentication mode, enter the key chain to be digested.
- Distribute-list In—Select to configure filtering on RIP incoming routes for one or more specified IP addresses in the Access List Name. If this field is enabled, select the Access List Name below.
- Access List Name—Select the Access List name (which includes a list of IP addresses) of RIP incoming routes filtering for a specified IP interface.
- Distribute-list Out—Select to configure filtering on RIP outgoing routes for one or more specified IP addresses in the Access List Name. If this field is enabled, select the Access List Name below.
- Access List Name—Select the Access List name (which includes a list of IP addresses) of RIP outgoing routes filtering for a specified IP interface.

Step 3 Click **Apply**. The settings are written to the Running Configuration file.

RIPv2 Statistics

To view the RIP statistical counters for each IP address:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **RIPv2** > **RIPv2 Statistics**.

The following fields are displayed:

- IP Interface—IP interface defined on the Layer 2 interface.
- Bad Packets Received—Specifies the number of bad packets identified by RIP on the IP interface.

- Bad Routes Received—Specifies the number of bad routes received and identified by RIP on the IP interface. Bad routes mean that the route parameters are incorrect. For example, the IP destination is a Broadcast address, or the metric is 0 or greater than 16.
- Update Sent—Specifies the number of packets sent by RIP on the IP interface.

Step 2 To clear all interface counters, click **Clear All Interface Counters**.

RIPv2 Peer Router Database

To view the RIP Peers (neighbors) database:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **RIPv2** > **RIPv2 Peer Router Database**.

The following fields are displayed for the peer router database:

- Router IP Address—IP interface defined on the Layer 2 interface.
- Bad Packets Received—Specifies the number of bad packets identified by RIP on the IP interface.
- Bad Routes Received—Specifies the number of bad routes received and identified by RIP on the IP interface. Bad routes mean that the route parameters are incorrect. For example, the IP destination is a Broadcast, or the metric is 0 or greater than 16.
- Last Updated—Indicates that the last time RIP received RIP routes from the remote IP address.

Step 2 To clear all counters, click **Clear All Interface Counters**.

Access List

Access lists consists of permit and/or deny statements that filter traffic on a device. These statements are executed in a top down fashion. As traffic encounters the access list, the access list is parsed top to bottom, looking for a match. The first match encountered will determine if the traffic is permitted or denied. Therefore, the order of your access list statements is extremely important. Access list should be built from most specific to least specific. This will keep unintentional matching to a minimum. If no match is found, there is an implicit "deny everything" at the end of all access list statements.

Access lists are an integral part of working with switches, and they are vital to security.

Access List Settings

To set the global configuration of an access list, follow these steps:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **Access List** > **Access List Settings**.

Step 2 To add a new Access List, click **Add** to open the Add Access List page and enter the following fields:

- Name—Define a name for the access list.
- Source IPv4 Address—Enter the source IPv4 address. The following options are available:

- Any—All IP addresses are included.
- User Defined—Enter an IP address.

- Source IPv4 Mask—Enter the source IPv4 address mask type and value. The following options are available:
  - Network mask—Enter the network mask.
  - Prefix length—Enter the prefix length.

- Action—Select an action for the access list. The following options are available:
  - Permit—Permit entry of packets from one or more IP addresses in the access list.
  - Deny—Reject entry of packets from one or more IP addresses in the access list.

Step 3 Click **Apply**. The settings are written to the Running Configuration file.

Source IPv4 Address List

To populate an access list with IP addresses, complete the following:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **Access List** > **Source IPv4 Address List**.

Step 2 To modify the parameters of an access list, click **Add** and modify any of the following fields:

- Access List Name—Name of the access list.
- Source IPv4 Address—Source IPv4 address. The following options are available:
  - Any—All IP addresses are included.
  - User defined—Enter an IP address.

- Source IPv4 Mask—Source IPv4 address mask type and value. The following options are available:
  - Network mask—Enter the network mask (for example 255.255.0.0).
  - Prefix length—Enter the prefix length.

- Action—Action for the access list. The following options are available:
  - Permit—Permit entry of packets from one or more IP addresses in the access list.
  - Deny—Reject entry of packets from one or more IP addresses in the access list.

Step 3 Click **Apply**. The settings are written to the Running Configuration file.

VRRP

Note The VRRP feature is only available on the Cisco 550x series switches.

VRRP is an election and redundancy protocol that dynamically assigns the responsibility of a virtual router to one of the physical routers on a LAN. This increase the availability and reliability of routing paths in the network.

In VRRP, one physical router in a virtual router is elected as the stack active unit, with the other physical router of the same virtual router acting as backups in case the stack active unit fails. The physical routers are referred as VRRP routers.

The default gateway of a participating host is assigned to the virtual router instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. The physical router that is forwarding packets at any given time is called the active router.

VRRP also enables load sharing of traffic. Traffic can be shared equitably among available routers by configuring VRRP in such a way that traffic to and from LAN clients are shared by multiple routers.

Virtual Routers

VRRP properties can be configured and customized in the VRRP Virtual Routers page.

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **VRRP** > **Virtual Routers**.

The virtual routers are displayed. The fields are described in the Add page except for the following fields that are generated by the system:

- Active/Standby Status—Displays whether the virtual router is a Active, Standby or neither of these.
- Active Primary Address—Displays the IP address of the active router.
- Preempt Mode—Is Preemptive feature enabled or disabled.

Step 2 To add a virtual router, click **Add**.

Step 3 Enter the following fields:

- Interface—Interface on which virtual router is defined.
- Virtual Router Identifier—User-defined number identifying virtual router.
- Description—User-defined string identifying virtual router.
- Status—Select to enable VRRP on the device.
- Version—Select the version of VRRP to be used on this router.
- IP Address Owner—If Yes is checked, this indicates that the IP address of the device is the IP address of the virtual router. Select the IP addresses of the owner from the Available IP Address list and move it to the Owner IP Address list.

  If No is checked, you must enter one or more addresses of the virtual router in the Virtual Router IP Addresses field. If multiple IP addresses are added here, separate them as follows: 1.1.1.1, 2.2.2.2.

- Source IP Address—Select the IP address to be used in VRRP messages. The default source IP address is the lowest of the IP addresses defined on the interface.
- Priority—If this device is the owner, this field gets the value 255, and this value can't be changed. If not, enter the priority of this device, based on its ability to function as an active unit. 100 is the default for a non-owner device.
- Preempt Mode—Select one of the following options:
  - True—When a VRRP router is configured with higher priority than the current active unit is up, it replaces the current active unit.
  - False—Even if a VRRP router with a higher priority than the current active unit is up, it doesn't replace the current active unit. Only the original active unit (when it becomes available) replaces the standby unit.
- Accept Control Mode—Select one of the following options:
  - Drop—The virtual router in Active state drops packets addressed to the Virtual router IP address if it's not the address owner.
  - Accept—The virtual router in Active state accepts packets addressed to the IP address of the Virtual router as its own even if it's not the address owner.
- IP SLA Track—Select to enable tracking of connectivity from the router to the next hop of the default route.
- Tracking Object—Enter the number of the SLA track that verifies the connectivity. This value was entered in the SLA Tracks page.
- Decrement—If the track object state is down, the VRRP priority of the router is decremented by this value.
- Advertisement Interval—Enter how frequently advertisement packets are sent.

Note If these parameters are changed (Edit), the virtual router is modified and a new message is sent with the new parameters.

Step 4 To add your new router to the list, click **Apply**.

Step 5 To see further information about a virtual router, select it and click **Details**.

The following fields are displayed for the selected virtual router:

- Interface—The Layer 2 interface (port, LAG, or VLAN) on which the virtual router is defined.
- Virtual Router Identifier—The virtual router identification number.
- Virtual Router MAC Address—The virtual MAC address of the virtual router
- Virtual Router IP Address Table—IP addresses associated with this virtual router.
- Description—The virtual router name.
- Additional Status
  - Version—The virtual router version
  - Status—Is VRRP enabled.
  - IP Address Owner—The owner of the IP address of the virtual router
  - Active/Standby Status—Is the virtual router the active or standby unit.

- Skew Time—Time used in calculation of active down interval
- Active Down Interval—Length of time that active unit has been down.
- Preempt Mode—Is Preempt mode enabled.
- Accept/Control Mode—Displays either Drop/Accept.

- Tracker Parameters
  - Tracker Object—Displays number of the SLA track that verifies the connectivity.
  - Decrement—If the track object state is down, the VRRP priority of the router is decremented by this value.
  - State—Displays whether route is Up or Down.
  - Current Priority—Displays priority of the router.

- My Parameters (of virtual router selected)
  - Priority—Priority of this virtual router's device, based on its ability to function as the active unit.
  - Advertisement Interval—Advertisment time interval .
  - Source IP Address—IP address to be used in VRRP messages.

- Active Parameters
  - Priority—255
  - Advertisement Interval—Advertisment time interval.
  - Source IP Address—IP address to be used in VRRP messages.

VRRP Statistics

To view VRRP statistics and to clear interface counters:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **VRRP**> **VRRP Statistics**.

The following fields are displayed for every interface on which VRRP is enabled:

- Interface—Displays the interface on which VRRP is enabled.
- Invalid Checksum—Displays number of packets with invalid checksums.
- Invalid Packet Length—Displays number of packets with invalid packet lengths.
- Invalid TTL—Displays number of packets with invalid time-to-live values.
- Invalid VRRP Packet Type—Displays number of packets with invalid VRRP packet types.
- Invalid VRRP ID—Displays number of packets with invalid VRRP IDs.
- Invalid Protocol Number—Displays number of packets with invalid protocol numbers.

- Invalid IP List—Displays number of packets with invalid IP lists.
- Invalid Interval—Displays number of packets with invalid intervals.
- Invalid Authentication—Displays number of packets that failed authentication.

Step 2 Select an interface.

Step 3 Click **Clear Interface Counters** to clear the counters for that interface.

Step 4 Click **Clear All Interface Counters** to clear all the counters.

SLA

Note The SLA feature is only available on the Cisco 550x series switches.

Object tracking of IP Service Level Agreements (SLAs) operations allows tracking clients to track the output from IP SLAs objects and use the provided information to trigger an action.

Cisco IOS IP SLAs is a network performance measurement and diagnostics tool that uses active monitoring. Active monitoring is the generation of traffic in a reliable and predictable manner to measure network performance. software uses IP SLAs to collect real-time metrics such as response time, network resource availability, application performance, jitter (interpacket delay variance), connect time, throughput, and packet loss. These metrics can be used for troubleshooting, for proactive analysis before problems occur, and for designing network topologies.

ICMP-Echo Operations

IP SLA ICMP-Echo operations can be configured in this page. These operations will be executed according to the frequency entered.

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **SLA** > **ICMP-Echo Operations**.

The ICMP-Echo operations are displayed (some fields described in the Add page):

- State—Displays either Pending or Scheduled, as described in the Overview above.
- Return Code—Displays either OK or Error, as described in the Overview above.

Step 2 To add a new operation, click **Add**.

Step 3 Enter the following fields:

- Operation Number—Enter an unused number.
- Operation State—Select one of the following options:
  - Pending—Operation is not activated.
  - Scheduled—Operation is activated.

ICMP-Echo Parameters

- Operation Target—Select how the operation target is defined:
  - By IP—Enter the operation target's IP address.
  - By host name—Enter the operation target's host name.

  Note If the IP SLA operation is for the Static Routes feature, the operation target is the IP address of the host in the remote network defined by the static route.

- Source Definition—If this field is not defined, the operation selects the source IP address nearest to the destination. To define this field, select from one of the following options:
  - Auto—The source interface is based on Forwarding Table information.
  - By address— Specify a different source IP address.
- Next Hop IP Address—Select **None** or User-Defined. If User-Defined is selected, enter the next hop IP address. This parameter should be defined only for IP SLAs operations to be used the static routes.
- Request Data Size—Enter the request packet data size for an ICMP Echo operation. This data size is the payload portion of the ICMP packet, which makes a 64-byte IP packet.
- Frequency—Enter the frequency with which the SLA operation is carried out (packets are sent). This value must be larger than the Timeout.
- Timeout—Enter the amount of time an IP SLA operation waits for a response to its request packet. It is recommend that the value of the milliseconds argument be based on the sum of the maximum round-trip time (RTT) value for the packets and the processing time of the IP SLAs operation.

Step 4 Click **Apply** to save the settings.

SLA Tracks

SLA tracks can be configured in this page. SLA tracks are used to track IP SLA return codes and set a state of up or down, accordingly.

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **SLA** > **SLA Tracks**.

The SLA Track objects are displayed (some fields are described in the Add page):

- State—Displays one of the following states:
  - Down—There's no connectivity to the route (packet returned Error return code).
  - Up—There's connectivity to the route (packet returned OK return code).
- Operation Type—Can only display ICMP-Echo.
- Delay Interval Remainder (Sec)—How much of Delay period remains.

Step 2 To add a new object, click **Add**.

Step 3 Enter the following fields:

- Track Number—Enter an unused number.
- Operation Number—Select an SLA operation from a list.
- Up Delay—Specifies a time in seconds to delay state changes from down to up:
  - None—Change the state of the track immediately.
  - Delay Period—Change the state of the track after this delay period.
- Down Delay—Specifies a time in seconds to delay state changes from Up to Down:
  - None—Change the state of the track immediately.
  - Delay Period—Change the state of the track after this delay period.

Step 4 Click **Apply** to save the settings.

ICMP-Echo Statistics

To view SLA statistics.

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **SLA** > **ICMP-Echo Statistics**.

Step 2 Enter the following fields:

- SLA Operation—Select one of the operations that were previously defined.
- Refresh Rate—Select the how often the statistics should be refreshed. The available options are:
  - No Refresh—Statistics are not refreshed.
  - 15 Sec—Statistics are refreshed every 15 seconds.
  - 30 Sec—Statistics are refreshed every 30 seconds.
  - 60 Sec—Statistics are refreshed every 60 seconds.

Step 3 View the following fields:

- Operation Successes—Number of times the SLA track echo was successful.
- Operation Failures—Number of times the SLA track echo was successful.
- ICMP-Echo Requests—Number of request packets that were sent.
- ICMP-Echo Replies—Number of reply packets that were received.
- ICMP-Echo Errors—Number of error packets that were received.

To refresh these counters click:

- Clear Counters—Clears counters for selected operation.
- Clear All Operations Counters—Clears counters for all operations.

- Refresh—Refresh the counters.

ARP

The device maintains an ARP (Address Resolution Protocol) table for all known devices that reside in the IP subnets directly connected to it. A directly connected IP subnet is the subnet to which an IPv4 interface of the device is connected. When the device is required to send/route a packet to a local device, it searches the ARP table to obtain the MAC address of the device. The ARP table contains both static and dynamic addresses. Static addresses are manually configured and don't age out. The device creates dynamic addresses from the ARP packets it receives. Dynamic addresses age out after a configured time.

Note The mapping information is used for routing and to forward generated traffic.

To define the ARP tables, complete the following steps:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **ARP**.

Step 2 Enter the parameters.

- ARP Entry Age Out—Enter the number of seconds that dynamic addresses can remain in the ARP table. A dynamic address age out after the time it's in the table exceeds the ARP Entry Age Out time. When a dynamic address ages out, it's deleted from the table, and only returns when it's relearned.
- Clear ARP Table Entries—Select the type of ARP entries to be cleared from the system.
  - All—Deletes all of the static and dynamic addresses immediately
  - Dynamic—Deletes all of the dynamic addresses immediately
  - Static—Deletes all of the static addresses immediately
  - Normal Age Out—Deletes dynamic addresses based on the configured ARP Entry Age Out time.

Step 3 Click **Apply.** The ARP global settings are written to the Running Configuration file.

The ARP table displays the following fields:

- Interface—The IPv4 Interface of the directly connected IP subnet where the IP device resides.
- IP Address—The IP address of the IP device.
- MAC Address—The MAC address of the IP device.
- Status—Whether the entry was manually entered or dynamically learned.

Step 4 Click **Add**.

Step 5 Enter the parameters:

- IP Version—The IP address format supported by the host. Only IPv4 is supported.

- Interface—An IPv4 interface can be configured on a port, LAG, or VLAN. Select the desired interface from the list of configured IPv4 interfaces on the device.
- IP Address—Enter the IP address of the local device.
- MAC Address—Enter the MAC address of the local device.

Step 6 Click **Apply**. The ARP entry is saved to the Running Configuration file.

ARP Proxy

The Proxy ARP technique is used by the device on a given IP subnet to answer ARP queries for a network address that isn't on that network.

Note The ARP proxy feature is only available when the device is in L3 mode.

The ARP Proxy is aware of the destination of traffic, and offers another MAC address in reply. Serving as an ARP Proxy for another host effectively directs LAN traffic destination to the host. The captured traffic is then typically routed by the Proxy to the intended destination by using another interface, or by using a tunnel. The process in which an ARP-query-request for a different IP address, for proxy purposes, results in the node responding with its own MAC address is sometimes referred to as publishing.

To enable ARP Proxy on all IP interfaces, complete the following steps:

Step 1 Click **IP Configuration**> **IPv4 Management and Interfaces** >**ARP Proxy**.

Step 2 Select **ARP Proxy** to enable the device to respond to ARP requests for remotely-located nodes with the device MAC address.

Step 3 Click **Apply**. The ARP proxy is enabled, and the Running Configuration file is updated.

UDP Relay/IP Helper

Switches don't typically route IP Broadcast packets between IP subnets. However, this feature enables the device to relay specific UDP Broadcast packets, received from its IPv4 interfaces, to specific destination IP addresses.

To configure the relaying of UDP packets received from a specific IPv4 interface with a specific destination UDP port, add a UDP Relay:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **UDP Relay/IP Helper**.

Step 2 Click **Add.**

Step 3 Select the Source IP Interface to where the device is to relay UDP Broadcast packets based on a configured UDP destination port. The interface must be one of the IPv4 interfaces configured on the device.

Step 4 Enter the UDP Destination Port number for the packets that the device is to relay. Select a well-known port from the drop-down list, or click the port radio button to enter the number manually.

Step 5 Enter the Destination IP Address that receives the UDP packet relays. If this field is 0.0.0.0, UDP packets are discarded. If this field is 255.255.255.255, UDP packets are flooded to all IP interfaces.

Step 6 Click **Apply**. The UDP relay settings are written to the Running Configuration file.

DHCP Snooping/Relay

This section covers Dynamic Host Configuration Protocol (DHCP) Snooping/Relay. A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently. By contrast, relay agents receive DHCP messages and then generate a new DHCP message to send on another interface.

DHCP snooping is a layer 2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. The fundamental use case for DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients.

Properties

DHCP Relay transfers DHCP packets to the DHCP server. The device can transfer DHCP messages received from VLANs that do not have IP addresses. Whenever DHCP Relay is enabled on a VLAN without an IP address, Option 82 is inserted automatically.

TO set the DHCP Snooping/Relay properties, complete the followin steps:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Snooping/Relay** > **Properties**.

Step 2 Configure the following fields:

- DHCP Relay—Select to enable DHCP Relay
- DHCP Snooping Status—Select to enable DHCP Snooping.
- Option 82 Pass Through—Select to leave foreign Option 82 information when forwarding packets.
- Verify MAC Address—Select to verify that the source MAC address of the Layer 2 header matches the client hardware address as appears in the DHCP Header (part of the payload) on DHCP untrusted ports.
- Backup Database—Select to back up the DHCP Snooping Binding database on the device's flash memory.

Step 3 Click **Apply**. The settings are written to the Running Configuration file.

Step 4 To define a DHCP server, click **Add**. The Add DHCP Server dialog appears, with the IP version indicated.

Step 5 Enter the IP address of the DHCP server and click **Apply**. The settings are written to the Running Configuration file.

Option 82 Settings

Option 82 (DHCP Relay Agent Information Option) passes port and agent information to a central DHCP server, indicating where an assigned IP address physically connects to the network. The main goal of option 82 is to help to the DHCP server select the best IP subnet (network pool) from which to obtain an IP address.

Option 82, when enabled, applies to DHCP Relay interface with IP address and DHCP Snooping. Even if Option 82 isn't enabled, and if DCHP relay is enabled on VLAN without an IP address, option 82 information will be inserted to DHCP packets received on this VLAN.

To configure the status on the device and the format of the Option 82 data within the DHCP message, follow these steps:

Step 1 Click **IP Configuration >IPv4 Management and Interfaces> DHCP Snooping/Relay**> **Option 82 Settings**.

Enter the following fields:

-
- Option 82 Insertion—Check Enable to insert Option 82 information into packets.
- Numeric Token Format—Select Hexadecimal or Ascii as needed. This parameter defines the format to use for the following tokens:
  - $int-ifindex$
  - $int-portid$
  - $switch-moduleid$
  - $vlan-id$

  For example, the $vlan-id$ token, where VLAN ID is 35. VLAN ID 35 can be sent either as Hexa byte of 0x23 or ASCII representation of value of 0x3335. See the full information on the various tokens in the following table.

Step 2 Enter the Circuit-ID Template. Select **Use Default** to use the default Circuit-ID. Select **User Defined** to configure the Circuit-ID. Use the text box to enter the Circuit-ID template. The template is a string of free text and pre-defined tokens (see table below). You can enter tokens manually, or use the drop-down to select a token from the list of available tokens and add it to the Circuit-ID text by clicking the arrow button. Use the Preview button to view actual Sub option byte content and text representation of the selected sub-option.

Step 3 Enter the Remote-ID Template in the same way as the Circuit-ID Template, using the related text box and drop-down list.

Note The **Total Sub-Option Payload** shows the dynamically updated number of reserved byte count of the payload of both sub-options. The payload must not exceed 247. Byte count is based on the reserved length of the tokens included in the sub-option, plus the number of free text chars used in the sub-option.

Step 4 Click **Apply**. The settings are written to the Running Configuration file.

These are the tokens that are available from the drop-down box.

Option	Description	Reserved bytes	Bytes used in Hex format	Byt ASC
$int-ifindex$	The ifIndex of the interface on which the DHCP client request was received. Value is taken from the ifIndex field of the ifTable MIB entry	4	2	4
$int-portid$	The interface number relative to the specific unit (standalone or stacking unit). For physical interfaces this value begins with 1 for the 1st port on a specific unit, 2 for the 2nd port on that unit, until N for last port on that unit. For LAG interfaces the value is determined globally (and not based on specific unit), according to the LAG ID. For example, 1,2,3….	2	1	2
$int-name$	The full name of the interface, upon which the DHCP client request was received. The name is based on the interface full name format as used by CLI when configuring or displaying information for this interface	32	NA	Act for repr the nan lim byt
$int-abrvname$	The abbreviated name of the interface, upon which the DHCP client request was received. This parameter is based on the abbreviated interface name format as used by CLI when configuring or displaying information for this interface.	8	NA	
$int-desc-16$	Up to 16 (first) bytes of the interface description - for the interface, upon which the DHCP client packet was received. The value for this variable is taken from the description added by the user to the interface using the interface level "description" command. Max number of bytes to use is 16 (first bytes) - even if description is longer than 16 bytes. For interfaces without a user-defined description - the interface abbreviated interface name format is used.	16	NA	Act for repr the des the rese

Option	Description	Reserved bytes	Bytes used in Hex format
$int-desc-32$	Up to 32 (first) bytes of the interface description - for the interface, upon which the DHCP client packet was received. The value for this variable is taken from the description added by the user to the interface using the interface level "description" command. Max number of bytes to use is 32 (1st bytes) - even if description is longer than 32 bytes. For interfaces without user-defined description - the interface abbreviated interface name format is used.	32	NA
$int-desc-64$	The full interface description (up to 64 bytes) - for the interface, upon which the DHCP client packet was received. The value for this variable is taken from the description added by the user to the interface using the interface level "description" command. For interfaces without user-defined description - the interface abbreviated interface name format is used.	64	NA
$int-mac$	The MAC address of the physical interface upon which the DHCP client request was received. The format of this field is always HEX format, with no delimiter (for example, 000000112205).	6	6
$switch-mac$	The base MAC address of the device inserting the option 82 (the relay agent). The format of this field is always HEX format, with no delimiter (for example, 000000112200).	6	6
$switch-hostname-16$	Up to the first 16 bytes of the device hostname.	16	NA
$switch-hostname-32$	Up to the first 32 bytes of the device hostname.	32	NA
$switch-hostname-58$	The full hostname of the device.	58	NA
$switch-module-id$	The unit ID of the unit upon which the DHCP client request was received. In standalone systems ID is always equal 1.	2	1
$vlan-id$	The VLAN ID of the VLAN upon the DHCP client request was received. Values 1-4094	4	2

Option	Description	Reserved bytes	Bytes used in Hex format	Byt ASC
$vlan-name-16$	Up to the first 16 bytes of the VLAN name, for the VLAN upon which the DHCP client request was received. If a name isn't configure for the specified VLAN, the value is taken from the relevant VLAN ifDescr MIB field of ifTable MIB entry.	16	NA	Act for repr the (up rese
$vlan-name-32$	The full VLAN name of the VLAN upon the DHCP client request was received. If a name is configure for the specified VLAN, the value is taken from the relevant ifDescr MIB field of ifTable MIB entry.	32	NA	

Note The total reserved byte count of the payload of both sub-options must not exceed 247. The byte count isn't updated dynamically and shown at the bottom of the screen. Byte count is based on the reserved length (see above) of the tokens included in the sub-option, plus the number of free text chars used in the sub-option.

Interface Settings

DHCP Relay and Snooping can be enabled on any interface or VLAN. For DHCP relay to be functional, an IP address must be configured on the VLAN or interface.

DHCPv4 Relay Overview

DHCP Relay relays DHCP packets to the DHCP server. The device can relay DHCP messages received from VLANs that do not have IP addresses. Whenever DHCP Relay is enabled on a VLAN without an IP address, Option 82 is inserted automatically. This insertion is in the specific VLAN and does not influence the global administration state of Option 82 insertion.

DHCPv4 Snooping Overview

DHCP snooping provides a security mechanism to prevent receiving false DHCP response packets and to log DHCP addresses. It does this by treating ports on the device as either trusted or untrusted. A trusted port is a port that is connected to a DHCP server and is allowed to assign DHCP addresses. DHCP messages received on trusted ports are allowed to pass through the device. An untrusted port is a port that is not allowed to assign DHCP addresses. By default, all ports are considered untrusted until you declare them trusted (in the Interface Settings page).

To enable DHCP Snooping/Relay on specific interfaces, follow these steps:

Step 1 Click **IP Configuration > IPv4 Management and Interfaces > DHCP Snooping/Relay > Interface Settings.**

Step 2 To enable DHCP Relay or DHCP Snooping on an interface, click **ADD**.

Step 3 Select DHCP Relay or DHCP Snooping or both to enable.

Step 4 Click **Apply**. The settings are written to the Running Configuration file.

DHCP Snooping Trusted Interfaces

Packets from untrusted ports/LAGs are checked against the DHCP Snooping Binding database. By default, interfaces are untrusted. To designate an interface as trusted, follow these steps:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Snooping/Relay** > **DHCP Snooping Trusted Interfaces.**

Step 2 Select the interface and click **Edit**.

Step 3 Select **Trusted Interface** (Yes for trusted or No for untrusted).

Step 4 Click **Apply** to save the settings to the Running Configuration file.

DHCP Snooping Binding Database

Note the following points about maintenance of the DHCP Snooping Binding database:

- The device doesn't update the DHCP Snooping Binding database when a station moves toanother interface.
- If a port is down, the entries for that port aren't deleted.
- When DHCP Snooping is disabled for a VLAN, the binding entries that collected for that VLAN are removed.
- If the database is full, DHCP Snooping continue to forward packets but new entries aren't created. Note that if the IP source guard and/or ARP inspection features are active, the clients that aren't written in the DHCP Snooping Binding database aren't been able to connect to the network.

To add entries to the DHCP Snooping Binding database, follow these steps:

Step 1 Click **IP Configuration > IPv4 Management and Interfaces > DHCP Snooping/Relay > DHCP Snooping Binding Database**.

To see a subset of entries in the DHCP Snooping Binding database, enter the relevant search criteria in the filter and click **Go**.

Step 2 To add an entry, click **Add**. The supported address type is IPv4.

Step 3 Enter the fields:

- VLAN ID—VLAN on which packet is expected.
- MAC Address—MAC address of packet.
- IP Address—IP address of packet.
- Interface—Unit/Slot/Interface on which packet is expected.
- Type—The possible field values are:
  - Dynamic—Entry has limited lease time.
  - Static—Entry was statically configured.

- Lease Time—If the entry is dynamic, enter the amount of time that the entry is to be active in the DHCP Database. If there's no Lease Time, check Infinite.)

Step 4 Click **Apply**. The settings are defined, and the device is updated.

DHCP Server

The DHCP Server feature enables you to configure the device as a DHCPv4 server. A DHCPv4 server is used to assign IPv4 address and other information to another device (DHCP client) The DHCPv4 server allocates IPv4 addresses from a user-defined pool of IPv4 addresses.

These can be in the following modes:

- Static Allocation—The hardware address or client identifier of a host is manually mapped to an IP address.
- Dynamic Allocation—A client obtains a leased IP address for a specified period of time (that can be infinite). If the DHCP client does not renew the allocated IP Address, the IP address is revoked at the end of this period, and the client must request another IP address.

DHCP Server Properties

To configure the device as a DHCPv4 server, follow these steps:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Server** > **Properties**.

Step 2 Select **Enable** to configure the device as a DHCP server.

Step 3 Click **Apply**. The device immediately begins functioning as a DHCP server. However, it does not assign IP addresses to clients until a pool is created.

Network Pools

When the device is serving as a DHCP server, one or more pools of IP addresses must be defined, from which the device allocates IP addresses to DHCP clients. Each network pool contains a range of addresses that belong to a specific subnet. These addresses are allocated to various clients within that subnet.

When a client requests an IP address, the device as DHCP server allocates an IP address according to the following:

- Directly Attached Client—The device allocates an address from the network pool whose subnet matches the subnet configured on the device's IP interface from which the DHCP request was received.

  If the message arrived directly (not via DHCP Relay) the pool is a Local pool and belongs to one of IP subnets defined on the input layer 2 interface. In this case, the IP mask of the pool equals to the IP mask of the IP interface and the minimum and maximum IP addresses of the pool belong to the IP subnet.

- Remote Client—The device takes an IP address from the network pool with the IP subnet that matches the IP address of the DHCP relay agent.

  If the message arrived via DHCP relay, the address used belongs to the IP subnet specified by minimum IP address and IP mask of the pool. That pool is a remote pool.

Up to 16 network pools can be defined.

To create a pool of IP addresses, and define their lease durations, follow these steps:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Server** > **Network Pools**.

The previously defined network pools are displayed. These fields are described below in the Add page. The following field is displayed (but not in the Add page):

- Number of Leased Addresses—Number of addresses in the pool that have been assigned (leased).

Step 2 Click **Add** to define a new network pool. Note that you either enter the Subnet IP Address and the Mask, or enter the Mask, the Address Pool Start and Address Pool End.

Step 3 Enter the fields:

- Pool Name—Enter the pool name.
- Subnet IP Address—Enter the subnet in which the network pool resides.
- Mask—Enter one of following:
  - Network Mask—Check and enter the pool's network mask.
  - Prefix Length—Check and enter the number of bits that comprise the address prefix.
- Address Pool Start—Enter the first IP address in the range of the network pool.
- Address Pool End—Enter the last IP address in the range of the network pool.
- Lease Duration—Enter the amount of time a DHCP client can use an IP address from this pool. You can configure a lease duration of up to 49,710 days or an infinite duration.
  - Infinite—The duration of the lease is unlimited.
  - Days—The duration of the lease in number of days The ranges is 0–49,710 days.
  - Hours—The number of hours in the lease A days value must be supplied before an hours value can be added.
  - Minutes—The number of minutes in the lease A days value and an hours value must be added before a minutes value can be added.
- Default Router IP Address (Option 3)—Enter the default router for the DHCP client.
- Domain Name Server IP Address (Option 6)—Select one of the devices DNS servers (if already configured) or select **Other** and enter the IP address of the DNS server available to the DHCP client.
- Domain Name (Option 15)—Enter the domain name for a DHCP client.
- NetBIOS WINS Server IP Address (Option 44)—Enter the NetBIOS WINS name server available to a DHCP client.
- NetBIOS Node Type (Option 46)—Select how to resolve the NetBIOS name. Valid node types are:
  - Hybrid—A hybrid combination of b-node and p-node is used. When configured to use h-node, a computer always tries p-node first and uses b-node only if p-node fails. This is the default.
  - Mixed—A combination of b-node and p-node communications is used to register and resolve NetBIOS names. M-node first uses b-node; then, if necessary, p-node. M-node is typically not the best choice for larger networks because its preference for b-node. Broadcasts increase network traffic.

- Peer-to-Peer—Point-to-point communications with a NetBIOS name server are used to register and resolve computer names to IP addresses.
- Broadcast—IP Broadcast messages are used to register and resolve NetBIOS names to IP addresses.

- SNTP Server IP Address (Option 4)—Select one of the device's SNTP servers (if already configured) or select **Other** and enter the IP address of the time server for the DHCP client.
- File Server IP Address (siaddr)—Enter the IP address of the TFTP/SCP server from which the configuration file is downloaded.
- File Server Host Name (sname/Option 66)—Enter the name of the TFTP/SCP server.
- Configuration File Name (file/Option 67)—Enter the name of the file that is used as a configuration file.

Step 4 Click **Apply**. The Running Configuration file is updated.

Excluded Addresses

By default, the DHCP server assumes that all pool addresses in a pool may be assigned to clients. A single IP address or a range of IP addresses can be excluded. The excluded addresses are excluded from all DHCP pools.

To define an excluded address range, follow these steps:

Step 1 Click **IP Configuration** > **> IPv4 Management and Interfaces** > **DHCP Server** > **Excluded Addresses**.

The previously defined excluded IP addresses are displayed.

Step 2 To add a range of IP addresses to be excluded, click **Add**, and enter the fields:

- Start IP Address—First IP address in the range of excluded IP addresses.
- End IP Address—Last IP address in the range of excluded IP addresses.

Step 3 Click **Apply**. The Running Configuration file is updated.

Static Hosts

You might want to assign some DHCP clients a permanent IP address that never changes. This client is then known as a static host. You can define up to 120 static hosts.

To manually allocate a permanent IP address to a specific client, complete the following steps:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Server** > **Static Hosts**.

The static hosts are displayed. The fields displayed are described in the Add page, except for the following:

- MAC Address/Client Identifier

Step 2 To add a static host, click **Add**, and enter the fields:

Option	Description
IP Address	Enter the IP address that was statically assigned to the host.
Host Name	Enter the host name, which can be a string of symbols and an integer.
Mask	Enter the static host's network mask. • Network Mask—Check and enter the static host's network mask. • Prefix Length—Check and enter the number of bits that comprise the address prefix.
Identifier Type	Set how to identify the specific static host. • Client Identifier—Enter a unique identification of the client specified in hexadecimal notation, such as: 01b60819681172. Or: • MAC Address—Enter the MAC address of the client. Enter either the Client Identifier or MAC Address, according to which type you selected.
Client Name	Enter the name of the static host, using a standard set of ASCII characters. The client name must not include the domain name.
Default Router IP Address (Option 3)	Enter the default router for the static host.
Domain Name Server IP Address (Option 6)	Select one of the devices DNS servers (if already configured) or select **Other** and enter the IP address of the DNS server available to the DHCP client.
Domain Name (Option 15)	Enter the domain name for the static host.
NetBIOS WINS Server IP Address (Option 44)	Enter the NetBIOS WINS name server available to the static host.
NetBIOS Node Type (Option 46)	Select how to resolve the NetBIOS name. Valid node types are: • Hybrid—A hybrid combination of b-node and p-node is used. When configured to use h-node, a computer always tries p-node first and uses b-node only if p-node fails. This is the default. • Mixed—A combination of b-node and p-node communications is used to register and resolve NetBIOS names. M-node first uses b-node; then, if necessary, p-node. M-node is typically not the best choice for larger networks because its preference for b-node. Broadcasts increases network traffic. • Peer-to-Peer—Point-to-point communications with a NetBIOS name server are used to register and resolve computer names to IP addresses. • Broadcast—IP Broadcast messages are used to register and resolve NetBIOS names to IP addresses.

Option	Description
SNTP Server IP Address (Option 4)	Select one of the device's SNTP servers (if already configured) or select **Other** and enter the IP address of the time server for the DHCP client.
File Server IP Address (siaddr)	Enter the IP address of the TFTP/SCP server from which the configuration file is downloaded.
File Server Host Name (sname/Option 66)	Enter the name of the TFTP/SCP server.
Configuration File Name (file/Option 67)	Enter the name of the file that is used as a configuration file.

Step 3 Click **Apply**. The Running Configuration file is updated.

DHCP Options

When the device is acting as a DHCP server, the DHCP options can be configured using the HEX option. A description of these options can be found in RFC2131. The configuration of these options determines the reply that is sent to DHCP clients whose packets include a request (using option 55) for the configured DHCP options. Example: The DHCP option 66 is configured with the name of a TFTP server in the DHCP Options page. When a client DHCP packet is received containing option 66, the TFTP server is returned as the value of option 66.

To configure one or more DHCP options, follow these steps:

Step 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Server** > **DHCP Options**.

The previously configured DHCP options are displayed.

Step 2 To configure an option that has not been configured yet, enter the field:

- DHCP Server Pool Name equals to—Select one of the pool of network addresses defined in the Network Pools, on page 24 and click **Go** to filter by that pool of network addresses.

Step 3 Click **Add** and enter the fields:

- Pool Name—Displays the name of the pool name for which code is being defined.
- Code—Enter the DHCP option code.
- Type—The radio buttons for this field, change according to the type of the DHCP option's parameter. Select one of the following codes and enter the value for the DHCP options parameter:
  - Hex—Select if you want to enter the hex value of the parameter for the DHCP option. A hex value can be provided in place of any other type of value. For instance, you can provide a hex value of an IP address instead of the IP address itself.

    No validation is made of the hex value, therefore if you enter a HEX value, which represents an illegal value, no error is provided, and the client might not be able to handle the DHCP packet from the server.
  - IP—Select if you want to enter an IP address when this is relevant for the DHCP option selected.

- IP List—Enter list of IP addresses separated by commas.
- Integer—Select if you want to enter an integer value of the parameter for the DHCP option selected.
- Boolean—Select if the parameter for the DHCP option selected is Boolean.

- Boolean Value—If the type was Boolean, select the value to be returned: True or False.
- Value If the type isn't Boolean, enter the value to be sent for this code.
- Description—Enter a text description for documentation purposes.

Step 4 Click **Apply**. The Running Configuration file is updated.

Address Binding

Use the Address Binding page to view and remove the IP addresses allocated by the device and their corresponding MAC addresses.

To view and/or remove address bindings, complete the following steps:

Step 1 Click **IP Configuration** > **> IPv4 Management and Interfaces** > **DHCP Server** > **Address Binding**.

The following fields for the address bindings are displayed:

- IP Address—The IP addresses of the DHCP clients.
- Address Type—Whether the address of the DHCP client appears as a MAC address or using a client identifier.
- MAC Address/Client Identifier—A unique identification of the client specified as a MAC Address or in hexadecimal notation, e.g., 01b60819681172.
- Lease Expiration—The lease expiration date and time of the host's IP address or Infinite is such was the lease duration defined.
- Type—The manner in which the IP address was assigned to the client. The possible options are:
  - Static—The hardware address of the host was mapped to an IP address.
  - Dynamic—The IP address, obtained dynamically from the device, is owned by the client for a specified time. The IP address is revoked at the end of this period, when the client must request another IP address.
- State—The possible options are:
  - Allocated—IP address has been allocated. When a static-host is configured, its state is allocated.
  - Declined—IP address was offered but not accepted, therefore it's not allocated.
  - Expired—The lease of the IP address has expired.
  - Pre-Allocated—An entry is in preallocated state from the time between the offer and the time that the DHCP ACK is sent from the client. Then it becomes allocated.

Step 2 Click **Delete**. The Running Configuration file is updated.

IPv6 Management and Interfaces

The Internet Protocol version 6 (IPv6) is a network-layer protocol for packet-switched internetworks. IPv6 was designed to replace IPv4, the predominantly deployed Internet protocol. IPv6 introduces greater flexibility in assigning IP addresses, because the address size increases from 32-bit to 128-bit addresses. IPv6 addresses are written as eight groups of four hexadecimal digits, for example FE80:0000:0000:0000:0000:9C00:876A:130B. The abbreviated form, in which a group of zeroes can be left out, and replaced with '::', is also acceptable, for example, FE80::9C00:876A:130B.

IPv6 Global Configuration

IPv6 nodes require an intermediary mapping mechanism to communicate with other IPv6 nodes over an IPv4-only network. This mechanism, called a tunnel, enables IPv6-only hosts to reach IPv4 services, and enables isolated IPv6 hosts and networks to reach an IPv6 node over the IPv4 infrastructure. Tunneling uses either an ISATAP or manual mechanism (see IPv6 Tunnel). Tunneling treats the IPv4 network as a virtual IPv6 local link, with mappings from each IPv4 address to a link local IPv6 address. The device detects IPv6 frames by the IPv6 Ethertype.

This section provides information for defining the device IPv6 addresses, either manually or by making the device a DHCP client. To define IPv6 global parameters and DHCPv6 client settings, follow these steps:

Step 1 Click **IP Configuration >IPv6 Management and Interfaces > IPv6 Global Configuration.**

Step 2 Enter values for the following fields:

- IPv6 Routing—Select to enable IPv6 routing. If this isn't enabled, the device acts as a host (not a router) and can receive management packets, but can't forward packets. If routing is enabled, the device can forward the IPv6 packets.

  Enabling IPv6 routing removes any address previously assigned to the device interface, via the auto-config operation, from an RA sent by a Router in the network.

- ICMPv6 Rate Limit Interval—Enter how often the ICMP error messages are generated.
- ICMPv6 Rate Limit Bucket Size—Enter the maximum number of ICMP error messages that can be sent by the device per interval.
- IPv6 Hop Limit—Enter the maximum number of intermediate routers on its way to the final destination to which a packet can pass. Each time a packet is forwarded to another router, the hop limit is reduced. When the hop limit becomes zero, the packet is discarded. This prevents packets from being transferred endlessly.
- DHCPv6 Client Settings
  - Unique Identifier (DUID) Format—This is the identifier of the DHCP client that is used by the DHCP server to locate the client. It can be in one of the following formats:

    Link-Layer—(Default). If you select this option, the MAC address of the device is used.

    Enterprise Number—If you select this option, enter the following fields.

- Enterprise Number—The vendors registered Private Enterprise number as maintained by IANA.
- Identifier—The vendor-defined hex string (up to 64 hex characters) If the number of the character isn't even, a zero is added at the right. Each 2 hex characters can be separated by a period or colon.

- DHCPv6 Unique Identifier (DUID)—Displays the identifier selected.

Step 3 Click **Apply**. The IPv6 global parameters and DHCPv6 client settings are updated.

IPv6 Interfaces

An IPv6 interface can be configured on a port, LAG, VLAN, loopback interface or tunnel.

To define an IPv6 interface, follow these steps:

Step 1 Click **IP Configuration > IPv6 Management and Interfaces > IPv6 Interfaces**.

Step 2 Enter the parameters.

- IPv6 Link Local Default Zone—Select to enable defining a default zone. This is an interface to be used to egress a link-local packet arriving without a specified interface or with its default zone 0.
- IPv6 Link Local Default Zone Interface—Select an interface to be used as a default zone. This can be a previously defined tunnel or other interface.

Step 3 Click **Apply** to configure default zone.

The IPv6 Interface Table is displayed along with the following field:

- Tunnel Type—Manual, 6–4 and ISATAP.

Step 4 Click **Add** to add a new interface on which interface IPv6 is enabled.

Step 5 Enter the fields:

- IPv6 Interface—Select a specific port, LAG, loopback interface or VLAN for the IPv6 address.

Step 6 To configure the interface as a DHCPv6 client, meaning to enable the interface to receive information from the DHCPv6 server, such as: SNTP configuration and DNS information, enter the DHCPv6 Client fields:

- DHCPv6 Client—Select to enable DHCPv6 Client (stateless and stateful) on the interface.
- Rapid Commit—Select to enable the use of the two-message exchange for address allocation and other configuration. If it's enabled, the client includes the rapid-commit option in a solicit message.
- Minimum Information Refresh Time—This value is used to put a floor on the refresh time value. If the server sends a refresh time option that is less than this value, this value is used instead. Select Infinite or User Defined to set a value.
- Information Refresh Time—This value indicates how often the device refreshes information received from the DHCPv6 server. If this option isn't received from the server, the value entered here is used. Select Infinite or User Defined to set a value.

Step 7 To configure additional IPv6 parameters, enter the following fields:

- IPv6 Address Auto Configuration—Select to enable automatic address configuration from router advertisements sent by neighbors.
- Number of DAD Attempts—Enter the number of consecutive neighbor solicitation messages that are sent while Duplicate Address Detection (DAD) is performed on the interface's Unicast IPv6 addresses. DAD verifies the uniqueness of a new Unicast IPv6 address before it's assigned. New addresses remain in a tentative state during DAD verification. Entering 0 in this field disables duplicate address detection processing on the specified interface. Entering 1 in this field indicates a single transmission without follow-up transmissions.
- Send ICMPv6 Messages—Enable generating unreachable destination messages.
- MLD Version—IPv6 MLD version.
- IPv6 Redirects—Select to enable sending ICMP IPv6 redirect messages. These messages inform other devices not to send traffic to the device, but rather to another device.

Step 8 Click **Apply** to enable IPv6 processing on the selected interface. Regular IPv6 interfaces have the following addresses automatically configured:

- Link local address using EUI-64 format interface ID based on a device's MAC address
- All node link local Multicast accdresses (FF02::1)
- Solicited-Node Multicasy address (format FF02::1:FFXX:X)

Step 9 Click **Restart** to initiate a refresh of the stateless information received from the DHCPv6 server.

Step 10 Click **IPv6 Address Table** to manually assign IPv6 addresses to the interface, if required.

Step 11 To add a tunnel, select an interface in the IPv6 Tunnel Table and click **IPv6 Tunnel**.

IPv6 Tunnels

Tunnels enable transmission of IPv6 packets over IPv4 networks. Each tunnel has a source IPv4 address and if it's a manual tunnel it also has a destination IPv4 address. The IPv6 packet is encapsulated between these addresses.

ISATAP Tunnels

The device supports a single Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnel. An ISATAP tunnel is a point-to-multi-point tunnel. The source address is the IPv4 address (or one of the IPv4 addresses) of the device. When configuring an ISATAP tunnel, the destination IPv4 address is provided by the router. Note that:

- An IPv6 link local address is assigned to the ISATAP interface. The initial IP address is assigned to the interface, which is then activated.
- If an ISATAP interface is active, the ISATAP router IPv4 address is resolved via DNS by using ISATAP-to-IPv4 mapping. If the ISATAP DNS record is not resolved, ISATAP host name-to-address mapping is searched in the host mapping table
- When the ISATAP router IPv4 address is not resolved via the DNS process, the ISATAP IP interface remains active. The system does not have a default router for ISATAP traffic until the DNS process is resolved.

To configure an IPv6 tunnel follow these steps:

Step 1 Click **IP Configuration > IPv6 Management and Interfaces > IPv6 Tunnel**.

Step 2 Enter the ISATAP parameters:

- Solicitation Interval—The number of seconds between ISATAP router solicitations messages, when no active ISATAP router is discovered. The interval can be the Default Value or a User Defined interval.
- Robustness—Used to calculate the interval for router solicitation queries. The bigger the number, the more frequent the queries. The interval can be the Default Value or a User Defined interval .

Note The ISATAP tunnel is not operational if the underlying IPv4 interface is not in operation.

Step 3 Click **Add**.

Note Manual and 6 to 4 tunnels are only relevant for the SG350XG/SX350X device and the Sx550 family of devices. For these devices the page displays the IPv6 Tunnel Table which displays and enables creating and configuring IPv6 tunnels (see steps below). The Sx350 and Sx350X support only ISATAP tunnels. For these devices the ISATAP tunnel is configured by clicking the Create ISATAP Tunnel button and entering information for the Source IPv4 Address and ISATAP Router Name fields. See the following explanations for these fields.

Step 4 Enter the following fields:

- Tunnel Name—Select a tunnel number.
- Tunnel Type—Select a tunnel type: Manual, 6 to 4 or ISATAP.
- Tunnel State (called State in the main page)—Select to enable the tunnel. If this tunnel is later shutdown, this fact will be indicated in this field.
- Link Status SNMP Traps—Select to enable generating a trap when the link status of a port is changed. If you are not interested in receiving such traps on specific ports (for example, ISP only needs traps on ports connected to its infrastructure, and does not need traps for the ports connected to the user's equipment), this feature can be disabled.
- Source (called Source Type in the main page)—Displays one of the following options:
  - Auto—Automatically selects the minimum IPv4 address from among all of its configured IPv4 interfaces as the source address for packets sent on the tunnel interface.

    If the minimum IPv4 address is removed from the interface (removed at all or moved to another interface), the next minimum IPv4 address is selected as the local IPv4 address.
  - IPv4 Address—Enter the IPv4 address of the interface that will be used as the source address of the tunnel.
  - Interface—Select the interface whose IPv4 address will be used as the source address of the tunnel.

    The main page has a column called Source Address. This presents the actual IP address that was selected based on the above selection.
- Destination—(For manual tunnel only) Select one of the following options to specify the destination address of the tunnel:
  - Host Name—DNS name of the remote host.
  - IPv4 Address—IPv4 address of the remote host.

- ISATAP Router Name— (For ISATAP tunnels only) Select one of the following options to configure a global string that represents a specific automatic tunnel router domain name.
  - Use Default—This is always ISATAP.
  - User Defined—Enter the router's domain name.

Step 5 Click **Apply**. The tunnel is saved to the Running Configuration file.

Note For a SG350XG/SX350X device and the 550 family of devices, to shut down a tunnel, click Edit and uncheck Tunnel State. To disable traps, click Edit and uncheck Link Status SNMP Traps.

IPv6 Addresses

To assign an IPv6 address to an IPv6 Interface, follow these steps:

Step 1 Click **IP Configuration > IPv6 Management and Interfaces > IPv6 Addresses**.

Step 2 To filter the table, select an interface name, and click **Go**. The interface appears in the IPv6 Address Table. These fields are described in the Add page except for the following fields:

- DAD Status—Displays whether Duplicate Access Detection is active or not and the DAD state. This column does not appear for interfaces of Tunnel type.
- Preferred Lifetime—Displays the entry preferred lifetime.
- Valid Lifetime—Displays the entry valid lifetime.
- Expiry Time—Displays the expiry time.

Step 3 Click **Add**.

Step 4 Enter values for the fields.

Option	Description
IPv6 Interface	Displays the interface on which the IPv6 address is to be defined. If an * is displayed, this means that the IPv6 interface is not enabled but has been configured.
IPv6 Address Type	Select the type of the IPv6 address to add. • Link Local—An IPv6 address that uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration. • Global—An IPv6 address that is a global Unicast IPV6 type that is visible and reachable from other networks. • Anycast—The IPv6 address is an Anycast address. This is an address that is assigned to a set of interfaces that typically belong to different nodes. A packet sent to an Anycast address is delivered to the closest interface—as defined by the routing protocols in use—identified by the Anycast address.

Option	Description
	Note Anycast cannot be used, if the IPv6 address is on an ISATAP interface.
IPv6 Address	In addition to the default link local and Multicast addresses, the device also automatically adds global addresses to the interface based on the router advertisements it receives. The device supports a maximum of 128 addresses at the interface. Each address must be a valid IPv6 address that is specified in hexadecimal format by using 16-bit values separated by colons.
Prefix Length	The length of the Global IPv6 prefix is a value from 0-128 indicating the number of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
EUI-64	Select to use the EUI-64 parameter to identify the interface ID portion of the Global IPv6 address by using the EUI-64 format based on a device MAC address.

Step 5 Click **Apply**. The Running Configuration file is updated.

IPv6 Router Configuration

The following sections describe how to configure IPv6 routers. It covers the following topics:

Router Advertisement

A router advertisement packet contains various configurations for IPv6 hosts including the network part of the layer 3 IPv6 address required by hosts to communicate in the internet. Clients then generate the universally unique host part of the address and derive the complete address. This feature can be enabled or suppressed per interface, as follows:

Step 1 Click **IP Configuration** > **IPv6 Management and Interfaces** >**IPv6 Router Configuration** >**Router Advertisement**.

Step 2 To configure an interface listed in the Router Advertisement Table, select it and click **Edit**.

Step 3 Enter the following fields:

Option	Description
Suppress Router Advertisement	Select Yes to suppress IPv6 router advertisement transmissions on the interface.
Router Preference	Select either Low, Medium or High preference for the router. Router advertisement messages are sent with the preference configured in this field. If no preference is configured, they are sent with a medium preference.
Include Advertisement Interval Option	Select to indicate that an advertisement option will be used by the system. This option indicates to a visiting mobile node the interval at which that node may expect to receive router advertisements. The node may use this information in its movement detection algorithm.
Hop Limit	This is the value that the router advertises. If it's not zero, it's used as the hop limit by the host.

Option	Description
Managed Address Configuration Flag	Select this flag to indicate to attached hosts that they should use stateful auto configuration to obtain addresses. Hosts may use stateful and stateless address auto configuration simultaneously.
Other Stateful Configuration Flag	Other Stateful Configuration Flag—Select this flag to indicate to attached hosts that they should use stateful auto configuration to obtain other (non-address) information. **Note** If the Managed Address Configuration flag is set, an attached host can use stateful auto configuration to obtain the other (non-address) information regardless of the setting of this flag.
Neighbor Solicitation Retransmissions Interval	Enter the interval to determine the time between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor (User Defined), or select Use Default to use the system default (1000).
Maximum Router Advertisement Interval	Enter the maximum amount of time that can pass between router advertisements. The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if you configure the route as a default router by using this command. To prevent synchronization with other IPv6 nodes, the actual interval used is randomly selected from a value between the minimum and maximum values.
Minimum Router Advertisement Interval	Enter the minimum amount of time that can pass between router advertisements (User Defined) or select Use Default to user the system default. **Note** The minimum RA interval may never be more than 75% of the maximum RA interval and never less than 3 seconds.
Router Advertisement Lifetime	Enter the remaining length of time, in seconds, that this router remains useful as a default router. A value of zero indicates that it's no longer useful as a default router.
Reachable Time	Enter the amount of time that a remote IPv6 node is considered reachable (in milliseconds) (User Defined) or select the Use Default option to use the system default.

Step 4 Click **Apply** to save the configuration to the Running Configuration file.

IPv6 Prefixes

To define prefixes to be advertised on the interfaces of the device, follow these steps:

Step 1 Click **IP Configuration** > **IPv6 Management and Interfaces** > **IPv6 Router Configuration** > **IPv6 Prefixes**.

Step 2 If required, enable the Filter field and click **Go**. The group of interfaces matching the filter are displayed.

Step 3 To add an interface, click **Add.**

Step 4 Select the required IPv6 Interface on which a prefix is to be added.

Step 5 Enter the following fields:

Option	Description
Prefix Address	The IPv6 network. This argument must be in the form documented in RFC 4293 where the address is specified in hexadecimal—using 16-bit values between colons.
Prefix Length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
Prefix Advertisement	Select to advertise this prefix.
Valid Lifetime	The remaining length of time, in seconds, that this prefix will continue to be valid, i.e., time until invalidation. The address generated from an invalidated prefix should not appear as the destination or source address of a packet. • Infinite—Select this value to set the field to 4,294,967,295, which represents infinity. • User Defined—Enter a value.
Preferred Lifetime	The remaining length of time, in seconds, that this prefix will continue to be preferred. After this time has passed, the prefix should no longer be used as a source address in new communications, but packets received on such an interface are processed as expected. The preferred-lifetime must not be larger than the valid-lifetime. • Infinite—Select this value to set the field to 4,294,967,295, which represents infinity. • User Defined—Enter a value.
Auto Configuration	Enable automatic configuration of IPv6 addresses using stateless auto configuration on an interface and enable IPv6 processing on the interface. Addresses are configured depending on the prefixes received in Router Advertisement messages.
Prefix Status	Select one of the following options: • Onlink—Configures the specified prefix as on-link. Nodes sending traffic to addresses that contain the specified prefix consider the destination to be locally reachable on the link. An onlink prefix is inserted into the routing table as a connected prefix (L-bit set). • No-Onlink—Configures the specified prefix as not onlink. A no onlink prefix is inserted into the routing table as a connected prefix but advertised with a L-bit clear. • Offlink—Configures the specified prefix as offlink. The prefix will be advertised with the L-bit clear. The prefix will not be inserted into the routing table as a connected prefix. If the prefix is already present in the routing table as a connected prefix (for example, because the prefix was also configured by adding an IPv6 address), it will be removed.

Step 6 Click **Apply** to save the configuration to the Running Configuration file.

IPv6 Default Router List

The IPv6 Default Router List page enables configuring and viewing the default IPv6 router addresses. This list contains the routers that are candidates to become the device default router for non-local traffic (it may

be empty). The device randomly selects a router from the list. The device supports one static IPv6 default router. Dynamic default routers are routers that have sent router advertisements to the device IPv6 interface.

When adding or deleting IP addresses, the following events occur:

- When removing an IP interface, all the default router IP addresses are removed. Dynamic IP addresses can't be removed.
- An alert message appears after an attempt is made to insert more than a single user-defined address.
- An alert message appears when attempting to insert a non-link local type address, meaning 'fe80:'.

To define a default router, complete the following:

Step 1 Click **IP Configuration** > **IPv6 Management and Interfaces** > **IPv6 Default Router List**.

This page displays the following fields for each default router:

- Outgoing Interface—Outgoing IPv6 interface where the default router resides.
- Default Router IPv6 Address—Link local IP address of the default router.
- Type—The default router configuration that includes the following options:
  - Static—The default router was manually added to this table through the Add button.
  - Dynamic—The default router was dynamically configured.
- Metric—Cost of this hop.

Step 2 Click **Add** to add a static default router.

Step 3 Enter the following fields:

- Next Hop Type—The IP address of the next destination to which the packet is sent. This is composed of the following:
  - Global—An IPv6 address that is a global Unicast IPV6 type that is visible and reachable from other networks.
  - Link Local—An IPv6 interface and IPv6 address that uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Point to Point—A point-to-point tunnel. Supported if IPv6 routing tunnels are supported.
- Outgoing Interface—Displays the outgoing Link Local interface.
- Default Router IPv6 Address—The IP address of the static default router
- Metric—Enter the cost of this hop.

Step 4 Click **Apply**. The default router is saved to the Running Configuration file.

IPv6 Neighbors

The IPv6 Neighbors page enables configuring and viewing the list of IPv6 neighbors on the IPv6 interface. The IPv6 Neighbor Table (also known as IPv6 Neighbor Discovery Cache) displays the MAC addresses of the IPv6 neighbors that are in the same IPv6 subnet as the device. This is the IPv6 equivalent of the IPv4 ARP Table. When the device needs to communicate with its neighbors, the device uses the IPv6 Neighbor Table to determine the MAC addresses based on their IPv6 addresses.

This page displays the neighbors that automatically detected or manually configured entries. Each entry displays to which interface the neighbor is connected, the neighbor's IPv6 and MAC addresses, the entry type (static or dynamic), and the state of the neighbor.

To define IPv6 neighbors, complete the following steps:

Step 1 Click **IP Configuration** > **IPv6 Management and Interfaces** > **IPv6 Neighbors**.

You can select an option to clear some or all of the IPv6 addresses in the IPv6 Neighbors Table.

- Static Only—Deletes the static IPv6 address entries.
- Dynamic Only—Deletes the dynamic IPv6 address entries.
- All Dynamic & Static—Deletes the static and dynamic address entries IPv6 address entries.

The following fields are displayed for the neighboring interfaces:

- Interface—Neighboring IPv6 interface type.
- IPv6 Address—IPv6 address of a neighbor.
- MAC Address—MAC address mapped to the specified IPv6 address.
- Type—Neighbor discovery cache information entry type (static or dynamic).
- State—Specifies the IPv6 neighbor status. The values are:
  - Incomplete—Address resolution is working. The neighbor has not yet responded.
  - Reachable—Neighbor is known to be reachable.
  - Stale—Previously-known neighbor is unreachable. No action is taken to verify its reachability until traffic must be sent.
  - Delay—Previously-known neighbor is unreachable. The interface is in Delay state for a predefined Delay Time. If no reachability confirmation is received, the state changes to Probe.
  - Probe—Neighbor is no longer known to be reachable, and Unicast Neighbor Solicitation probes are being sent to verify the reachability.
- Router—Specifies whether the neighbor is a router (Yes or No).

Step 2 To add a neighbor to the table, click **Add**.

Step 3 The following fields are displayed:

- Interface—Displays the neighboring IPv6 interface to be added.
- IPv6 Address—Enter the IPv6 network address assigned to the interface. The address must be a valid IPv6 address.

- MAC Address—Enter the MAC address mapped to the specified IPv6 address.

Step 4 Click **Apply**. The Running Configuration file is updated.

Step 5 To change the type of an IP address from Static to Dynamic, select the address, click **Edit** and use the Edit IPv6 Neighbors page.

IPv6 Prefix List

Prefix lists are configured with permit or deny keywords to either permit or deny a prefix based on a matching condition. An implicit deny is applied to traffic that doesn't match any prefix-list entry. A prefix-list entry consists of an IP address and a bit mask. The IP address can be for a classful network, a subnet, or a single host route. The bit mask is a number 1–32.

Prefix lists are configured to filter traffic based on a match of an exact prefix length or a match within a range when the ge and le keywords are used.

To create a prefix list, follow these steps:

Step 1 Click **IP Configuration** > **IPv6 Management and Interfaces** > **IPv6 Prefix List**.

Step 2 Click **Add**.

Step 3 Enter the following fields:

- List Name—Select one of the following options:
  - Use existing list—Select a previously defined list to add a prefix to it.
  - Create new list—Enter a name to create a new list.
- Sequence Number—Specifies the place of the prefix within the prefix list. Select one of the following options:
  - Auto Numbering—Puts the new IPV6 prefix after the last entry of the prefix list. The sequence number equals the last sequence number plus 5. If the list is empty the first prefix-list entry is assigned the number 5 and subsequent prefix list entries increment by 5.
  - User Defined—Puts the new IPV6 prefix into the place specified by the parameter. If an entry with the number exists, it's replaced by the new one.
- Rule Type—Enter the rule for the prefix list:
  - Permit—Permits networks that match the condition.
  - Deny—Denies networks that match the condition.
  - Description—Text
- IPv6 Prefix—IP route prefix.
- Prefix Length—IP route prefix length.
- Greater Than—Minimum prefix length to be used for matching. Select one of the following options:
  - No Limit—No minimum prefix length to be used for matching.

- User Defined—Minimum prefix length to be matched.

- Lower Than—Maximum prefix length to be used for matching. Select one of the following options:
  - No Limit—No maximum prefix length to be used for matching.
  - User Defined—Maximum prefix length to be matched.

- Description—Enter a description of the prefix list.

Step 4 Click **Apply** to save the configuration to the Running Configuration file.

IPv6 Access Lists

The IPv6 access list can be used in MLD Proxy > Global MLD Proxy Settings > SSM IPv6 Access List page.

To create an access list, complete the following steps:

Step 1 Click **IP Configuration > IPv6 Management and Interfaces > IPv6 Access List** . To see a subset of entries in the list, enter the relevant search criteria in the filter and click **Go**.

Step 2 To add a new Access List, click **Add** and enter the following fields:

- Access List Name—Select one of the following:
  - Use existing list—Select a previously-existing access list.
  - Create new list—Enter a name for the new access list.

- Source IPv6 Address—Enter the source IPv6 address. The following options are available:
  - Any—All IP addresses are included.
  - User Defined—Enter an IP address.

- Prefix length—Enter the source IPv6 prefix length:
- Action—Select an action for the access list. The following options are available:
  - Permit—Permit entry of packets from the IP address(es) in the access list.
  - Deny—Reject entry of packets from the IP address(es) in the access list.

Step 3 Click **Apply**. The settings are written to the Running Configuration file.

IPv6 Routes

The IPv6 Forwarding Table contains the various routes that have been configured. One of these routes is a default route (IPv6 address: 0) that uses the default router selected from the IPv6 Default Router List to send packets to destination devices that aren't in the same IPv6 subnet as the device. In addition to the default

route, the table also contains dynamic routes that are ICMP redirect routes received from IPv6 routers by using ICMP redirect messages. This could happen when the default router the device uses isn't the router for traffic to which the IPv6 subnets that the device wants to communicate.

To view IPv6 routes:

Click **IPv6 Configuration** > **IPv6 Management and Interfaces**>**IPv6 Routes**.

This page displays the following fields:

- IPv6 Prefix—IP route address prefix for the destination IPv6 subnet address
- Prefix Length—IP route prefix length for the destination IPv6 subnet address It's preceded by a forward slash.
- Outgoing Interface—Interface used to forward the packet.
- Next Hop—Type of address to which the packet is forwarded. Typically, this is the address of a neighboring router. It can be one of the following types.
  - Link Local—An IPv6 interface and IPv6 address that uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—An IPv6 address that is a global Unicast IPV6 type that is visible and reachable from other networks.
  - Point-to-Point—A Point-to-point tunnel
- Metric—Value used for comparing this route to other routes with the same destination in the IPv6 router table All default routes have the same value.
- Lifetime—Time period during which the packet can be sent, and resent, before being deleted.
- Route Type—How the destination is attached, and the method used to obtain the entry. The following values are:
  - S (Static)—Entry was manually configured by a user.
  - I (ICMP Redirect)—Entry is an ICMP redirect dynamic route received from an IPv6 router by using ICMP redirect messages.
  - ND (Router Advertisement)—Entry is taken from a router advertisement message.

Step 1 To add a new route, click **Add** and enter the fields described above. In addition, enter the following field:

- IPv6 Address—Add the IPv6 address of the new route.

Step 2 Click **Apply** to save the changes.

DHCPv6 Relay

DHCPv6 Relay is used for relaying DHCPv6 messages to DHCPv6 servers. It's defined in RFC 3315.

When the DHCPv6 client isn't directly connected to the DHCPv6 server, a DHCPv6 relay agent (the device) to which this DHCPv6 client is directly-connected encapsulates the received messages from the directly connected DHCPv6 client, and forwards them to the DHCPv6 server.

In the opposite direction, the relay agent decapsulates packets received from the DHCPv6 server and forwards them, towards the DHCPv6 client.

The user must configure the list DHCP servers to which packets are forwarded. Two sets of DHCPv6 servers can be configured:

- Global Destinations—Packets are always relayed to these DHCPv6 servers.
- Interface List—This is a per-interface list of DHCPv6 servers. When a DHCPv6 packet is received on an interface, the packet is relayed both to the servers on the interface list (if it exists) and to the servers on the global destination list.

Global Destinations

To configure a list of DHCPv6 servers to which all DHCPv6 packets are relayed, complete the following steps:

Step 1 Click **IP Configuration**> **IPv6 Management and Interfaces** > **DHCPv6 Relay** > **Global Destinations**.

Step 2 To add a default DHCPv6 server, click **Add**.

Step 3 Enter the fields:

- IPv6 Address Type—Enter the type of the destination address to which client messages are forwarded. The address type can be Link Local, Global, or Multicast (All_DHCP_Relay_Agents_and_Servers).
- DHCPv6 Server IP Address—Enter the address of the DHCPv6 server to which packets are forwarded.
- IPv6 Interface—Enter the destination interface on which packets are transmitted when the address type of the DHCPv6 server is Link Local or Multicast. The interface can be a VLAN, LAG, or tunnel.

Step 4 Click **Apply**. The Running Configuration file is updated.

Interface Settings

To enable the DHCPv6 Relay feature on an interface and to configure a list of DHCPv6 servers, follow these steps:

Step 1 Click **IP Configuration** > **IPv6 Management and Interfaces** > **DHCPv6 Relay** > **Interface Settings**.

Step 2 To enable DHCPv6 on an interface and optionally add a DHCPv6 server for an interface, click **Add**.

Enter the fields:

- Source Interface—Select the interface (port, LAG, VLAN, or tunnel) for which DHCPv6 Relay is enabled.
- Use Global Destinations Only—Select to forward packets to the DHCPv6 global destination servers only.
- IPv6 Address Type—Enter the type of the destination address to which client messages are forwarded. The address type can be Link Local, Global, or Multicast (All_DHCP_Relay_Agents_and_Servers).

- DHCPv6 Server IP Address—Enter the address of the DHCPv6 server to which packets are forwarded.
- Destination IPv6 Interface— Select the destination IPv6 Interface from the drop-down menu.

Step 3 Click **Apply**. The Running Configuration file is updated.

Policy-Based Routing

Policy-based Routing (PBR) provides a means for routing selected packets to a next hop address based on packet fields, using ACLs for classification. PBR lessens reliance on routes derived from routing protocols.

Route Maps

Route maps are the means used to configure PBR.

To add a route map, complete the following steps:

Step 1 Click **IP Configuration** > **Policy Based Routing** > **Route Maps**.

Step 2 Click **Add** and enter the parameters:

- Route Map Name—Select one of the following options for defining a route map:
  - Use existing map—Select a route map that was previously defined to add a new rule to it.
  - Create new map—Enter the name of a new route map.
- Sequence Number—Number that indicates the position/priority of rules in a specified route map. If a route map has more than one rule (ACL) defined on it, the sequence number determines the order in which the packets will be matched against the ACLs (from lower to higher number).
- Route Map IP Type—Select either IPv6 or IPv4 depending on the type of the next hop IP address.
- Match ACL—Select a previously defined ACL. Packets will be matched to this ACL.
- IPv6 Next Hop Type—If the next hop address is an IPv6 address, select one of the following characteristics:
  - Global—An IPv6 address that is a global Unicast IPV6 type that is visible and reachable from other networks.
  - Link Local—An IPv6 interface and IPv6 address that uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network.
  - Point to Point—A point-to-point tunnel.
- Interface—Displays the outgoing Link Local interface.
- Next Hop—IP address of the next hop router.

Step 3 Click **Apply**. The Running Configuration file is updated.

Route Map Binding

All packets coming in on an interface that is bound to a route map and match a route map rule are routed to the next hop defined in the rule.

To bind an interface to a route map, complete the following steps:

Step 1 Click **IP Configuration** > **Policy Based Routing** > **Route Map Binding**.

Step 2 Click **Add** and enter the parameters:

- Interface—Select an interface (with an ip address).
- Bound IPv4 Route Map—Select an IPv4 route map to bind to the interface.
- Bound IPv6 Route Map—Select an IPv6 route map to bind to the interface.

Step 3 Click **Apply**. The Running Configuration file is updated.

Policy-Based Routes

To view the route maps that defined, complete the following steps:

Step 1 Click **IP Configuration** > **Policy Based Routing** > **Policy Based Routes**.

Step 2 Previously-defined route maps are displayed:

- Interface Name—Interface on which route map is bound.
- Route Map Name—Name of route map.
- Route Map Status—Status of interface:
  - Active—Interface is up.
  - Interface Down—Interface is down.
- ACL Name—ACL associated with route map.
- Next Hop—Where packets matching route map will be routed.
- Next Hop Status—Reachability of next hop:
  - Active—The next hop IP address is reachable.
  - Unreachable—The status isn't active the next hop IP address isn't reachable.
  - Not Direct—The status isn't active because the next hop IP address isn't directly attached to a device subnet.

Domain Name System

The Domain Name System (DNS) translates domain names into IP addresses for the purpose of locating and addressing hosts.

As a DNS client, the device resolves domain names to IP addresses through the use of one or more configured DNS servers.

DNS Settings

Use the DNS Settings page to enable the DNS feature, configure the DNS servers and set the default domain used by the device. To configure the DNS Settings, follow these steps;

Step 1 Click **Configuration** > **DNS** > **DNS Settings**.

Step 2 In Basic Mode, enter the parameters:

- Server Definition—Select one of the following options for defining the DNS server:
  - By IP Address—IP Address will be entered for DNS server.
  - Disabled—No DNS server will be defined.
- Server IP Address—If you selected By IP Address above, enter the IP address of the DNS server.
- Default Domain Name—Enter the DNS domain name used to complete unqualified host names. The device appends this to all nonfully qualified domain names (NFQDNs) turning them into FQDNs.

  Note Don't include the initial period that separates an unqualified name from the domain name (like cisco.com).

Step 3 In Advanced Mode, enter the parameters.

- DNS—Select to designate the device as a DNS client, which can resolve DNS names into IP addresses through one or more configured DNS servers.
- Polling Retries—Enter the number of times to send a DNS query to a DNS server until the device decides that the DNS server doesn't exist.
- Polling Timeout—Enter the number of seconds that the device waits for a response to a DNS query.
- Polling Interval—Enter how often (in seconds) the device sends DNS query packets after the number of retries has been exhausted.
  - Use Default—Select to use the default value.

    This value = 2*(Polling Retries + 1)* Polling Timeout
  - User Defined—Select to enter a user-defined value.
- Default Parameters—Enter the following default parameters:
  - Default Domain Name—Enter the DNS domain name used to complete unqualified host names. The device appends this to all nonfully qualified domain names (NFQDNs) turning them into FQDNs.

Note Don't include the initial period that separates an unqualified name from the domain name (like cisco.com).

- DHCP Domain Search List—Click **Details** to view the list of DNS servers configured on the device.

Step 4 Click **Apply**. The Running Configuration file is updated.

The DNS Server Table displays the following information for each DNS server configured:

- DNS Server—The IP address of the DNS server.
- Preference—Each server has a preference value, a lower value means a higher chance of being used.
- Source—Source of the server's IP address (static or DHCPv4 or DHCPv6)
- Interface—Interface of the server's IP address.

Step 5 Up to eight DNS servers can be defined. To add a DNS server, click **Add.**

Step 6 Enter the parameters.

- IP Version—Select Version 6 for IPv6 or Version 4 for IPv4.
- IPv6 Address Type—Select the IPv6 address type (if IPv6 is used). The options are:
  - Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- Link Local Interface—If the IPv6 address type is Link Local, select the interface through which it's received.
- DNS Server IP Address—Enter the DNS server IP address.
- Preference—Select a value that determines the order in which the domains are used (from low to high). This effectively determines the order in which unqualified names are completed during DNS queries.

Step 7 Click **Apply**. The DNS server is saved to the Running Configuration file.

Search List

The search list can contain one static entry defined by the user in the DNS Settings, on page 46 page and dynamic entries received from DHCPv4 and DHCPv6 servers.

To view the domain names that have been configured on the device, click **IP Configuration** > **DNS** > **Search List**.

The following fields are displayed for each DNS server configured on the device.

- Domain Name—Name of domain that can be used on the device.
- Source—Source of the server's IP address (static or DHCPv4 or DHCPv6) for this domain.

- Interface—Interface of the server's IP address for this domain.
- Preference—This is the order in which the domains are used (from low to high). This effectively determines the order in which unqualified names are completed during DNS queries.

Host Mapping

Host name/IP address mappings are stored in the Host Mapping Table (DNS cache).

This cache can contain the following type of entries:

- Static Entries—These are mapping pairs that manually added to the cache. There can be up to 64 static entries.
- Dynamic Entries—Are mapping pairs that are either added by the system as a result of being used by the user, or an entry for each IP address configured on the device by DHCP. There can be 256 dynamic entries.

Name resolution always begins by checking static entries, continues by checking the dynamic entries, and ends by sending requests to the external DNS server. Eight IP addresses are supported per DNS server per host name.

To add a host name and its IP address, complete the following:

Step 1 Click **IP Configuration** > **DNS** > **Host Mapping**.

Step 2 If required, select **Clear Table** to clear some or all of the entries in the Host Mapping Table.

- Static Only—Deletes the static hosts.
- Dynamic Only—Deletes the dynamic hosts.
- All Dynamic & Static—Deletes the static and dynamic hosts.

The Host Mapping Table displays the following fields:

- Host Name—User-defined host name or fully qualified name.
- IP Address—The host IP address.
- IP Version—IP version of the host IP address.
- Type—Is a Dynamic or Static entry to the cache.
- Status—Displays the results of attempts to access the host.
  - OK—Attempt succeeded
  - Negative Cache—Attempt failed, don't try again.
  - No Response—There was no response, but system can try again in future.
- TTL (Sec)—If this is a dynamic entry, how long will it remain in the cache.
- Remaining TTL (Sec)—If this is a dynamic entry, how much longer will it remain in the cache.

Step 3 To add a host mapping, click **Add**.

Step 4 Enter the parameters.

- IP Version—Select Version 6 for IPv6 or Version 4 for IPv4.
- IPv6 Address Type—Select the IPv6 address type (if IPv6 is used). The options are:
  - Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- Link Local Interface—If the IPv6 address type is Link Local, select the interface through which it's received.
- Host Name—Enter a user-defined host name or fully qualified name. Host names are restricted to the ASCII letters A through Z (case-insensitive), the digits 0–9, the underscore, and the hyphen. A period (.) is used to separate labels.
- IP Address—Enter a single address or up to eight associated IP addresses (IPv4 or IPv6).

Step 5 Click **Apply**. The settings are saved to the Running Configuration file.