IPv6 Configuration

This chapter contains the following sections:

IPv6 Global Configuration

The Internet Protocol version 6 (IPv6) is a network-layer protocol for packet-switched internet works. 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 interface addresses can be configured manually by the user, or automatically configured by a DHCP server.

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 **IPv6 Configuration** > **IPv6 Global Configuration**.

Step 2 Enter values for the following fields:

- IPv6 Routing—Select **Enable** 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

The Internet Protocol version 6 (IPv6) is a network-layer protocol used for packet-switched internet communications.IPv6 was created to replace IPv4, the most widely used Internet protocol. Because the address size increases from 32-bit to 128-bit, IPv6 allows for greater flexibility in assigning IP addresses. IPv6 addresses are composed of eight groups of four hexadecimal digits, such as FE80:0000:0000:0000:0000:9C00:876A:130B.

To communicate with other IPv6 nodes over an IPv4-only network, IPv6 nodes require an intermediary mapping mechanism. This mechanism, known as a tunnel, allows IPv6-only hosts to access IPv4 services and isolated IPv6 hosts and networks to connect to an IPv6 node via the IPv4 infrastructure.

An IPv6 interface can be configured on a port, LAG, VLAN, loopback interface or tunnel. To define an IPv6 interface, follow these steps:

Note Tunnel interfaces are created in the IPv6 Tunnels, on page 4

To define an IPv6 interface, follow these steps:

Step 1 Click **IPv6 Configuration** > **IPv6 Interfaces**.

Step 2 Enter the parameters.

- IPv6 Link Local Default Zone—Select **Enable** 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 the default zone. The IPV6 Interface Table is displayed along with the following fields:

- Tunnel Type—N/A, 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 **Enable** to enable DHCPv6 Client (stateless and stateful) on the interface.
- Rapid Commit—Select **Enable** 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 **Enable** 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—Select the IPv6 MLD version.
- IPv6 Redirects—Select **Enable** 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 addresses (FF02::1)
- Solicited-Node Multicast address (format FF02::1:FFXX:X)

Step 9 Click **IPv6 Address Table** to manually assign IPv6 addresses to the interface, if required.

Step 10 To add a tunnel, select an interface in the IPv6 Tunnel Table and click **IPv6 Tunnel**.

Step 11 Click **Apply** to save the settings.

Step 12 Press **Restart** to initiate refresh of the stateless information received from the DHCPv6 server.

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.

Note The tunneling options will be displayed differently between the 10G SKUs and the non 10G SKUs.

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.

Additional Types of Tunnels

The following additional types of tunnels can be configured on the device:

Manual Tunnel

- 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.

This is a point-to-point definition. When creating a manual tunnel, you enter both the source IP address (one of the device's IP addresses) and the destination IPv4 address.

6 to 4 Tunnel

- 6 to 4 is an automatic tunneling mechanism that uses the underlying IPv4 network as a non-Broadcast multiple-access link layer for IPv6. Only one 6 to 4 tunnel is supported on a device.
- The 6 to 4 tunnel is supported only when IPv6 Forwarding is supported.
- IPv6 Multicast is not supported on the 6to4 tunnel interface
- The switch automatically creates a 2002::/16 on-link prefix on the 6to4 tunnel. The connected 2002::/16 route on the tunnel is added to the Routing Table as result of the on-link prefix creation
- When the tunnel mode is changed from 6to4 to another mode, the on-link prefix and connected routes are removed.
- When the next hop outgoing interface is the 6to4 tunnel, the IPv4 address of the next hop node is taken from the prefix 2002:WWXX:YYZZ::/48 of the IPv6 next hop IPv6 address, if it is global, and from the last 32 bits of the interface identifier of the IPv6next hop IPv6 address, if it is link local.

The following table summarizes tunnel support in the various devices:

Tunnel Type	C1200	C1300	C1300 Stacking	C1300 Stacking Supporting 10G
ISATAP	Supported	Supported	Supported	Supported
Manual	Not Supported	Not Supported	Not Supported	Supported - Up to 16 tunnels
Automatic 6to4 tunnel	Not Supported	Not Supported	Not Supported	Supported - a single 4-6 tunnel (with up to 16 tunnels in total)

To configure an IPv6 tunnel follow these steps:

Step 1 Click **IPv6 Configuration > IPv6 Tunnel**.

Step 2 Click **Create ISATAP Tunnel.**

Step 3 The Tunnel Number (1) and its Tunnel Type (ISATAP) are displayed.

Step 4 Enter the following fields

- Source IPv4 Address—Set the local (source) IPv4 address of a tunnel interface. The IPv4 address of the selected IPv4 interface is used to form part of the IPv6 address over the ISATAP tunnel interface. The IPv6 address has a 64-bit network prefix of fe80::, with the rest of the 64-bit formed by concatenating 0000:5EFE and the IPv4 address.
  - Auto—Automatically selects the lowest IPv4 address from among all of its configured IPv4 interfaces as the source address for packets sent on the tunnel interface.
  - Manual—Specifies the IPv4 address to use as the source address for packets sent on the tunnel interface. The local address of the tunnel interface is not changed when the IPv4 address is moved to another interface.

    Note If the device IPv4 address is changed, the local address of the tunnel interface is also changed

  - Interface—Specifies the interface

- ISATAP Router Name— 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 Enter the parameters:

- ISATAP 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.
- ISATAP 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 6 To delete an ISATAP tunnel, click **Delete ISATAP Tunnel**.

Step 7 Click **Apply** to save the ISATAP parameters to the Running Configuration file.

IPv6 Addresses

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

Step 1 Click **IPv6 Configuration** > **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:

- Address Source—Displays one of the address source types: DHCP, System or Static.
- 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

Option	Description
	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. **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 3-128 indicating the number of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
EUI-64	Select **Enable** 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 **IPv6 Configuration** > **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
Interface	Select the interface from the drop down list.
Suppress Router Advertisement	Select Yes to suppress IPv6 router advertisement transmissions on the interface.

Option	Description
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.
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 **IPv6 Configuration** > **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.**or if you like to edit an interface, select the interface and click **Edit**.

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 on-link. 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 off link. The prefix will be advertised with the L-bit clear. The prefix will not be inserted into the routing table as a connected prefix.

Option	Description
	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 **IPv6 Configuration** > **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.
  - Neighbor Discovery (ND)—The default router is set to ND. Neighbor Discovery Protocol is used to identify the relationships between the different neighboring devices in an IPv6 network.
- 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.

- 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 **IPv6 Configuration** > **IPv6 Neighbors**.

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

- 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.

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 Next, you will see the following settings displayed in the IPv6 Neighbor Table.

- 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, No, or N/A).

Step 6 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 **IPv6 Configuration** > **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 **IPv6 Configuration > 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 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.
- 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.
- Outgoing Interface—Interface used to forward the packet.
- 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 **IPv6 Configuration** > **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 **IPv6 Configuration** > **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.