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.

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 Relay

This section covers Dynamic Host Configuration Protocol (DHCP)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.

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 Relay** > **Properties**.

Step 2 Configure the following fields:

- DHCP Relay—Select to enable DHCP Relay

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.

Interface Settings

DHCP Relay 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 Relay > Interface Settings.**

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

Step 3 Select DHCP Relay to enable.

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

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.
- 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 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 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 6 Click **Apply** to save the ISATAP parameters to the Running Configuration file.

Step 7 To remove the ISATAP tunnel click the Delete ISATAP Tunnel button.

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. **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.
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.

Option	Description
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.

Option	Description
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.
- 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 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.

- 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.

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 20 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.