IPv4 Configuration

This chapter contains the following sections:

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:

Procedure

Step 1 Click **IPv4 Configuration** > **IPv4 Interface.**

Enter the following fields:

- IPv4 Routing—Check **Enable** 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.
- 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 seconds if DHCP Client is enabled on startup in order to give time to discover the 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** to add an IPv4 interface.

Step 4 Select the Interface: Select the port, LAG, VLAN, Loopback, as the interface associated with this IP configuration, and select an interface from the 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
  - *Renew IP Address Now—Check **Enable** to enable.
  - *Auto Configuration via DHCP—Display the status (Disabled or Enabled).

Note
*These only appear in the Edit pop-up option.

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

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:

Procedure

Step 1 Click **IPv4 Configuration** > **IPv4 Static Routes**.

Step 2 Click **Add** to add a new IPv4 static route or **Edit** to edit an existing one.

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 a 2-digit number specifying the prefix length (a number in the range of 0-32).
- 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, is 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.

The IPv4 Static Routes Table is displayed. The following field is displayed which isn't listed above.

- Outgoing Interface-Outgoing interface for this route.

IPv4 Forwarding Table

To view the IPv4 Forwarding Table, follow these steps:

Procedure

Step 1 Click **IPv4 Configuration** > **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.
  - Rejected—Route was rejected.
- 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:

Procedure

Step 1 Click **IPv4 Configuration** > **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, 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:

Procedure

Step 1 Click **IPv4 Configuration** > **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:

Procedure

Step 1 Click **IPv4 Configuration** > **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 DHCPRelay properties, complete the following steps:

Procedure

Step 1 Click **IPv4 Configuration** > **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 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.

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

Procedure

Step 1 Click **IPv4 Configuration > DHCP Relay > Interface Settings.**

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

Step 3 Select the interface and the feature to be enabled: **DHCP Relay**

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