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:

Step 1 Click **IPv4 Configuration** > **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
- Renew IP Address Now—Check **Enable** to enable.
- Auto Configuration via DHCP—Display the status (Disabled or Enabled).

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 standby active unit present, Cisco recommends configuring the IP address as a static address to prevent disconnecting from the network during a active stacking unit switchover. This is because when the standby active 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-enabled 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 **IPv4 Configuration** > **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 **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.
- Metric—Cost of this hop (a lower value is preferred).
- Administrative Distance—The administrative distance to the next hop (a lower value is preferred). This isn’t relevant for static routes.
- Outgoing Interface—Outgoing interface for this route.

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

RIPv2

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

Note This feature is only supported on firmware 3.1 and beyond.

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

The default gateway is a static route and it is advertised by RIP in the same way as all other static routers, if it is enabled by configuration. When IP Routing is enabled, RIP works fully. When IP Routing is disabled, RIP works in the passive mode, meaning that it only learns routes from the received RIP messages and does not send them.

Note To enable IP Routing, go to the IPv4 Interface page. The device supports RIP version 2, which is based on the following standards:

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

Received RIPv1 packets are dropped.

Enabling RIP

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

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

RIPv2 Properties

To enable or disable RIPv2 on the device, follow these steps:

Step 1 Click **IPv4 Configuration** > **RIPv2** > **RIPv2 Properties**.

Step 2 Select the following options as required:

- RIP—The following options are available:
  - Enable—Enable RIP.
  - Disable—Disable RIP. Disabling RIP deletes the RIP configuration on the system.
  - Shutdown—Set the RIP global state to shutdown.
- RIP Advertisement—Select to enable sending routing updates on all RIP IP interfaces.
- Default Route Advertisement—Select to enable sending the default route to the RIP domain. This route will serve as the default router.
- Default Metric—Enter the value of the default metric.

Step 3 Redistribute Static Route—Select to enable manually-defined (remote) routes.

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

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

Step 5 Redistribute Connected Route—Select to enable RIP routes that correspond to defined IP interfaces on which RIP is not enabled (defined locally).

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

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

- User Defined Metric—Enter the value of the metric.

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

RIPv2 Settings

To configure RIP on an IP interface, complete the following steps:

Step 1 Click **IPv4 Configuration** > **RIPv2** > **RIPv2 Settings**.

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

- IP Address—Select an IP interface defined on the Layer 2 interface.
- Shutdown—Keep RIP configuration on the interface, but set the interface to inactive.
- Passive—Specifies whether sending RIP route update messages is allowed on the specified IP interface. If this field isn’t enabled, RIP updates aren’t sent (passive).
- Offset—Specifies the metric number of the specified IP interface. This reflects the additional cost of using this interface, based on the speed of the interface.
- Default Route Advertisement—This option is defined globally in the RIPv2 Properties, on page 6 page. You can use the global definition or define this field for the specific interface. The following options are available:
  - Global—Use the global settings defined in the RIPv2 Properties. Screen
  - Disable—On this RIP interface, don’t advertise the default route.
  - Enable—Advertise the default route on this RIP interface.
- Default Route Advertisement Metric—Enter the metric for the default route for this interface.
- Authentication Mode—RIP authentication state (enable/disable) on a specified IP interface. The following options are available:
  - None—There’s no authentication performed.
  - Text—The key password entered below is used for authentication.
  - MD5—The MD5 digest of the key chain selected below is used for authentication.
- Key Password—If Text was selected as the authentication type, enter the password to be used.
- Key Chain—If MD5 was selected as the authentication mode, enter the key chain to be digested. This key chain is created as described in the section.
- Distribute-list In—Select to configure filtering on RIP incoming routes for one or more specified IP addresses in the Access List Name. If this field is enabled, select the Access List Name below.
- Access List Name—Select the Access List name (which includes a list of IP addresses) of RIP incoming routes filtering for a specified IP interface.
- Distribute-list Out—Select to configure filtering on RIP outgoing routes for one or more specified IP addresses in the Access List Name. If this field is enabled, select the Access List Name below.

- Access List Name—Select the Access List name (which includes a list of IP addresses) of RIP outgoing routes filtering for a specified IP interface.

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

RIPv2 Statistics

To view the RIP statistical counters for each IP address, complete the following steps:

Step 1 Click **IPv4 Configuration** > **RIPv2** > **RIPv2 Statistics**.

The following fields are displayed:

- IP Interface—IP interface defined on the Layer 2 interface.
- Bad Packets Received—Specifies the number of bad packets identified by RIP on the IP interface.
- Bad Routes Received—Specifies the number of bad routes received and identified by RIP on the IP interface. Bad routes mean that the route parameters are incorrect. For example, the IP destination is a Broadcast address, or the metric is 0 or greater than 16.
- Update Sent—Specifies the number of packets sent by RIP on the IP interface.

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

RIPv2 Peer Router Database

To view RIP Peer Router Databse, follow these steps:

Step 1 Click **IPv4 Configuration** > **RIPv2** > **RIPv2 Peer Router Database**.

The following fileds are displayed for the peer router database:

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

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

Access List

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

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

Access List Settings

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

Step 1 Click **IPv4 Configuration** > **Access List** > **Access List Settings**.

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

- Name—Define a name for the access list.
- Source IPv4 Address—Enter the source IPv4 address. The following options are available:
  - Any—All IP addresses are included.
  - User defined—Enter an IP address.
- Source IPv4 Mask—Enter the source IPv4 address mask type and value. The following options are available:
  - Network mask—Enter the network mask.
  - Prefix length—Enter the prefix length.
- Action—Select an action for the access list. The following options are available:
  - Permit—Permit entry of packets from one or more IP addresses in the access list.
  - Deny—Reject entry of packets from one or more IP addresses in the access list.

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

Source IPv4 Access List

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

Step 1 Click **IPv4 Configuration** > **Access List** > **Source IPv4 Access List**.

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

- Access List Name—Name of the access list.

- Source IPv4 Address—Source IPv4 address. The following options are available:
    - Any—All IP addresses are included.
    - User defined—Enter an IP address.
- Source IPv4 Mask—Source IPv4 address mask type and value. The following options are available:
    - Network mask—Enter the network mask (for example 255.255.0.0).
    - Prefix length—Enter the prefix length.
- Action—Action for the access list. The following options are available:
    - Permit—Permit entry of packets from one or more IP addresses in the access list.
    - Deny—Reject entry of packets from one or more IP addresses in the access list.

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

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 **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, 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 **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:

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 Snooping/Relay

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

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

Properties

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

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

Step 1 Click **IPv4 Configuration** > **DHCP Snooping/Relay** > **Properties**.

Step 2 Configure the following fields:

- DHCP Relay—Select to enable DHCP Relay

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

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

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

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

Option 82 Settings

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

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

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

Step 1 Click **IPv4 Configuration** > **DHCP Snooping/Relay** > **Option 82 Settings**.

Enter the following fields:

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

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

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

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

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

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

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

Option	Description	Reserved bytes	Bytes used in Hex format	Bytes used in ASCII format
$int-ifindex$	The ifIndex of the interface on which the DHCP client request was received. Value is taken from the ifIndex field of the ifTable MIB entry	4	2	4
$int-portid$	The interface number relative to the specific unit (standalone or stacking unit). For physical interfaces this value begins with 1 for the 1st port on a specific unit, 2 for the 2nd port on that unit, until N for last port on that unit. For LAG interfaces the value is determined globally (and not based on specific unit), according to the LAG ID. For example, 1,2,3….	2	1	2

Option	Description	Reserved bytes	Bytes used in Hex format	Bytes used in ASCII format
$int-name$	The full name of the interface, upon which the DHCP client request was received. The name is based on the interface full name format as used by CLI when configuring or displaying information for this interface	32	NA	Actual bytes used for the ASCII representation of the interface name (up to the limit of reserved bytes)
$int-abrvname$	The abbreviated name of the interface, upon which the DHCP client request was received. This parameter is based on the abbreviated interface name format as used by CLI when configuring or displaying information for this interface.	8	NA	

Option	Description	Reserved bytes	Bytes used in Hex format	Bytes used in ASCII format
$int-desc-16$	Up to 16 (first) bytes of the interface description - for the interface, upon which the DHCP client packet was received. The value for this variable is taken from the description added by the user to the interface using the interface level "description" command. Max number of bytes to use is 16 (first bytes) - even if description is longer than 16 bytes. For interfaces without a user-defined description - the interface abbreviated interface name format is used.	16	NA	Actual bytes used for the ASCII representation of the interface description (up to the limit of reserved bytes)

Option	Description	Reserved bytes	Bytes used in Hex format	Bytes used in ASCII format
$int-desc-32$	Up to 32 (first) bytes of the interface description - for the interface, upon which the DHCP client packet was received. The value for this variable is taken from the description added by the user to the interface using the interface level "description" command. Max number of bytes to use is 32 (1st bytes) - even if description is longer than 32 bytes. For interfaces without user-defined description - the interface abbreviated interface name format is used.	32	NA	Actual bytes used for the ASCII representation of the interface description (up to the limit of reserved bytes)
$int-desc-64$		64	NA	

Option	Description	Reserved bytes	Bytes used in Hex format	Bytes used in ASCII format
	The full interface description (up to 64 bytes) - for the interface, upon which the DHCP client packet was received. The value for this variable is taken from the description added by the user to the interface using the interface level "description" command. For interfaces without user-defined description - the interface abbreviated interface name format is used.			
$int-mac$	The MAC address of the physical interface upon which the DHCP client request was received. The format of this field is always HEX format, with no delimiter (for example, 000000112205).	6	6	NA
$switch-mac$	The base MAC address of the device inserting the option 82 (the relay agent). The format of this field is always HEX format, with no delimiter (for example, 000000112200).	6	6	NA

Option	Description	Reserved bytes	Bytes used in Hex format	Bytes used in ASCII format
$switch-hostname-16$	Up to the first 16 bytes of the device hostname.	16	NA	Actual bytes used for the ASCII representation of the hostname (up to the limit of reserved bytes)
$switch-hostname-32$	Up to the first 32 bytes of the device hostname.	32	NA	
$switch-hostname-58$	The full hostname of the device.	58	NA	
$switch-module-id$	The unit ID of the unit upon which the DHCP client request was received. In standalone systems ID is always equal 1.	2	1	2
$vlan-id$	The VLAN ID of the VLAN upon the DHCP client request was received. Values 1-4094	4	2	4

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

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

Interface Settings

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

DHCPv4 Relay Overview

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

DHCPv4 Snooping Overview

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

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

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

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

Step 3 Select the interface and the feature to be enabled: **DHCP Relay** or **DHCP Snooping** or both to enable.

Note The DHCP snooping setting is available only if there is an IP address configured on the selected interface.

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

DHCP Snooping Trusted Interfaces

Packets from untrusted ports/LAGs are checked against the DHCP Snooping Binding database (See DHCP Snooping Binding Database, on page 21). By default, interfaces are untrusted. To designate an interface as trusted, follow these steps:

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

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

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

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

DHCP Snooping Binding Database

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

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

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

Step 1 Click **IPv4 Configuration > DHCP Snooping Relay > DHCP Snooping Binding Database**.

The fields in the DHCP Snooping Binding Database are displayed for the IP Source Guard:

- Status
  - Active—IP Source Guard is active on the device.
  - Inactive—IP Source Guard isn't active on the device.
- Reason
  - No Problem
  - No Resource
  - No Snoop VLAN
  - Trust Port

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

Step 3 Enter the fields:

- VLAN ID—VLAN on which packet is expected.
- MAC Address—MAC address of packet.
- IP Address—IP address of packet.
- Interface—Unit/Slot/Interface on which packet is expected.
- Type—The possible field values are:
  - Dynamic—Entry has limited lease time.
  - Static—Entry was statically configured.
- Lease Time—If the entry is dynamic, enter the amount of time that the entry is to be active in the DHCP Database. If there’s no Lease Time, check Infinite.)

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

Step 5 Click **Clear Dynamic** to delete the configuration.

DHCP Server

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

These can be in the following modes:

- Static Allocation—The hardware address or client identifier of a host is manually mapped to an IP address.

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

DHCP Server Properties

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

Step 1 Click **IPv4 Configuration** > **DHCP Server** > **Properties** to display the Properties page.

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

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

Network Pools

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

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

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

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

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

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

Up to 16 network pools can be defined.

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

Step 1 Click **IPv4 Configuration** > **DHCP Server** > **Network Pools**.

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

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

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

Step 3 Enter the fields:

- Pool Name—Enter the pool name.
- Subnet IP Address—Enter the subnet in which the network pool resides.
- Mask—Enter one of following:
  - Network Mask—Check and enter the pool's network mask.
  - Prefix Length—Check and enter the number of bits that comprise the address prefix.
- Address Pool Start—Enter the first IP address in the range of the network pool.
- Address Pool End—Enter the last IP address in the range of the network pool.
- Lease Duration—Enter the amount of time a DHCP client can use an IP address from this pool. You can configure a lease duration of up to 49,710 days or an infinite duration.
  - Infinite—The duration of the lease is unlimited.
  - Days—The duration of the lease in number of days The ranges is 0–49,710 days.
  - Hours—The number of hours in the lease A days value must be supplied before an hours value can be added.
  - Minutes—The number of minutes in the lease A days value and an hours value must be added before a minutes value can be added.
- Default Router IP Address (Option 3)—Enter the default router for the DHCP client.
- Domain Name Server IP Address (Option 6)—Select one of the devices DNS servers (if already configured) or select **Other** and enter the IP address of the DNS server available to the DHCP client.
- Domain Name (Option 15)—Enter the domain name for a DHCP client.
- NetBIOS WINS Server IP Address (Option 44)—Enter the NetBIOS WINS name server available to a DHCP client.
- NetBIOS Node Type (Option 46)—Select how to resolve the NetBIOS name. Valid node types are:
  - Hybrid—A hybrid combination of b-node and p-node is used. When configured to use h-node, a computer always tries p-node first and uses b-node only if p-node fails. This is the default.
  - Mixed—A combination of b-node and p-node communications is used to register and resolve NetBIOS names. M-node first uses b-node; then, if necessary, p-node. M-node is typically not the best choice for larger networks because its preference for b-node. Broadcasts increase network traffic.
  - Peer-to-Peer—Point-to-point communications with a NetBIOS name server are used to register and resolve computer names to IP addresses.
  - Broadcast—IP Broadcast messages are used to register and resolve NetBIOS names to IP addresses.
- SNTP Server IP Address (Option 4)—Select one of the device's SNTP servers (if already configured) or select **Other** and enter the IP address of the time server for the DHCP client.
- File Server IP Address (siaddr)—Enter the IP address of the TFTP/SCP server from which the configuration file is downloaded.
- File Server Host Name (sname/Option 66)—Enter the name of the TFTP/SCP server.
- Configuration File Name (file/Option 67)—Enter the name of the file that is used as a configuration file.

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

Excluded Addresses

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

To define an excluded address range, follow these steps:

Step 1 Click **IPv4 Configuration** > **DHCP Server** > **Excluded Addresses**.

The previously defined excluded IP addresses are displayed.

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

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

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

Static Hosts

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

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

Step 1 Click **IPv4 Configuration** > **DHCP Server** > **Static Hosts**.

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

- MAC Address/Client Identifier

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

IP Address	Enter the IP address that was statically assigned to the host.
Host Name	Enter the host name, which can be a string of symbols and an integer.
Mask	Enter the static host’s network mask. • Network Mask—Check and enter the static host’s network mask. • Prefix Length—Check and enter the number of bits that comprise the address prefix.

Identifier Type	Set how to identify the specific static host. • Client Identifier—Enter a unique identification of the client specified in hexadecimal notation, such as: 01b60819681172. Or: • MAC Address—Enter the MAC address of the client. Enter either the Client Identifier or MAC Address, according to which type you selected.
Client Name	Enter the name of the static host, using a standard set of ASCII characters. The client name must not include the domain name.
Default Router IP Address (Option 3)	Enter the default router for the static host.
Domain Name Server IP Address (Option 6)	Select one of the devices DNS servers (if already configured) or select **Other** and enter the IP address of the DNS server available to the DHCP client.
Domain Name (Option 15)	Enter the domain name for the static host.
NetBIOS WINS Server IP Address (Option 44)	Enter the NetBIOS WINS name server available to the static host.
NetBIOS Node Type (Option 46)	Select how to resolve the NetBIOS name. Valid node types are: • Hybrid—A hybrid combination of b-node and p-node is used. When configured to use h-node, a computer always tries p-node first and uses b-node only if p-node fails. This is the default. • Mixed—A combination of b-node and p-node communications is used to register and resolve NetBIOS names. M-node first uses b-node; then, if necessary, p-node. M-node is typically not the best choice for larger networks because its preference for b-node. Broadcasts increases network traffic. • Peer-to-Peer—Point-to-point communications with a NetBIOS name server are used to register and resolve computer names to IP addresses. • Broadcast—IP Broadcast messages are used to register and resolve NetBIOS names to IP addresses.
SNTP Server IP Address (Option 4)	Select one of the device’s SNTP servers (if already configured) or select **Other** and enter the IP address of the time server for the DHCP client.
File Server IP Address (siaddr)	Enter the IP address of the TFTP/SCP server from which the configuration file is downloaded.
File Server Host Name (sname/Option 66)	Enter the name of the TFTP/SCP server.
Configuration File Name (file/Option 67)	Enter the name of the file that is used as a configuration file.

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

DHCP Options

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

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

Step 1 Click **IPv4 Configuration** > **DHCP Server** > **DHCP Options**.

The previously configured DHCP options are displayed.

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

- DHCP Server Pool Name equals to—Select one of the pool of network addresses defined in the Network Pools, on page 23 and click **Go** to filter by that pool of network addresses.

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

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

    No validation is made of the hex value, therefore if you enter a HEX value, which represents an illegal value, no error is provided, and the client might not be able to handle the DHCP packet from the server.
  - IP—Select if you want to enter an IP address when this is relevant for the DHCP option selected.
  - IP List—Enter list of IP addresses separated by commas.
  - Integer—Select if you want to enter an integer value of the parameter for the DHCP option selected.
  - Boolean—Select if the parameter for the DHCP option selected is Boolean.
- Boolean Value—If the type was Boolean, select the value to be returned: True or False.
- Value—If the type isn't Boolean, enter the value to be sent for this code.
- Description—Enter a text description for documentation purposes.

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

Address Binding

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

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

Step 1 Click **IPv4 Configuration** > **DHCP Server** > **Address Binding**.

The following fields for the address bindings are displayed:

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

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