General IP Configuration

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.

Policy-Based Routing

Policy-based routing is a process whereby the device puts packets through a route map before routing them. The route map determines which packets are routed to which device next. Policy-based Routing (PBR) provides a means for routing selected packets to a next hop address based on packet fields, using ACLs for classification. PBR lessens reliance on routes derived from routing protocols.

Route Maps

Route maps are the means used to configure PBR.

To add a route map, complete the following steps:

Procedure

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

Step 2 Click **Add** to add a route map or Edit to edit and existing one and configure the following parameters:

- Route Map Name—Select one of the following options for defining a route map:
  - Use existing map—Select a route map that was previously defined to add a new rule to it.
  - Create new map—Enter the name of a new route map.
- Sequence Number—Number that indicates the position/priority of rules in a specified route map. If a route map has more than one rule (ACL) defined on it, the sequence number determines the order in which the packets will be matched against the ACLs (from lower to higher number).

- Route Map IP Type—Select either IPv6 or IPv4 depending on the type of the next hop IP address.
- Match ACL—Select a previously defined ACL. Packets will be matched to this ACL.
- IPv6 Next Hop Type—If the next hop address is an IPv6 address, select one of the following characteristics:
    - Global—An IPv6 address that is a global Unicast IPV6 type that is visible and reachable from other networks.
    - Link Local—An IPv6 interface and IPv6 address that uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network.
- Interface—Displays the outgoing Link Local interface.
- Next Hop—IP address of the next hop router.

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

Route Map Binding

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

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

Procedure

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

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

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

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

Policy-Based Routes

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

Procedure

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

Step 2 Previously-defined route maps are displayed:

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

Domain Name System

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

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

DNS Settings

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

Procedure

Step 1 Click **General IP 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 non fully 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.

      The default 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 non fully 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 3 and dynamic entries received from DHCPv4 and DHCPv6 servers.

To view the domain names that have been configured on the device, click **General 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:

Procedure

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

Step 2 If required, select one of the following options from 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 this 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, do not 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** and configure the following:

- 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 4 Click **Apply**. The settings are saved to the Running Configuration file.

IPDT

Visible only in Advanced Mode.

Some networking applications (such as 802.1x-based dynamic ACL) require the knowledge of the host's IP address (or MAC to IP mapping) connected to its interfaces or VLAN. IP Device Tracking (IPDT) Provides this functionality.

IPDT is an application that can map the IP address of a host that is connected to the switch to the host MAC address. IPDT achieves this by snooping certain packets that are sent by the host. The IPDT application is not responsible for the actual snooping of the packets, this is performed by existing applications like ARP snooping or DHCP snooping. The IPDT is only responsible for creating and maintaining the IP to MAC-mapping database.

Applications that require the IP to MAC mapping are known because IPDT clients.

IPDT updates an IPDT client when an entry is added, modified, or removed. IPDT clients can also poll IPDT for the IP address of a host.

IP device tracking is enabled on an interface in one of the following 2 ways:

- The interface 802.1x Administrative Port Control setting is set to **Auto.**
- The user modifies the interface Maximum host value.

IP Device Tracking Mapping

Note This setting is only visible in Advanced Mode.

The IP Device Tracking (IPDT) Mapping table displays the hosts IP to MAC mapping as learned by the IP device tracking feature. To view the IPDT tracking mapping complete the following:

Procedure

Step 1 Navigate to **General IP Configuration > IPDT > IP Device Tracking Mapping**.

Step 2 In the IP Device Tracking Mapping Table, in the Filter section, select the Interface and click **Go**.

Step 3 The following is the information for each entry:

- IP Address – The IP address of the host.
- MAC Address – The MAC address of the host.
- VLAN – The VLAN that the host is a member of.
- Port – The interface the host is connected to.
- Probe Interval – The default probe interval (aging timer) is 30 seconds.
- State – The entry state:

  - Active – The host is responding to the probes sent by the device, and the interface is the up state.
  - In-active – the interface moved to the down state while the entry was in the active state.
- Source – The method used by IP Device tracking to learn the host IP address and MAC address. The supported values are ARP or DHCP.

Note In case the host is not responding to the probes sent by the device the entry will be removed from the table.

Step 4 Click **Clear Table** to clear the device tracking entries regardless of the applied filter.

IP Device Tracking Settings

Note This setting is available in Advanced Mode only.

The primary IPDT responsibility is to maintain track of linked hosts (MAC-IP address association). To accomplish this, it sends unicast Address Resolution Protocol (ARP) probes with a default interval of 30 seconds; these probes are sent to the MAC address of the host connected on the other side of the link, and use Layer 2 (L2) as the default source.

To configure the IPDT Tracking Settings, complete the following steps:

Procedure

Step 1 Navigate to **General Configuration** > **IPDT** > **IP Device Tracking Settings.**

Step 2 Next, configure the following parameters:

- Default Probe Count – The default number of probes that are sent after which a device tracking entry is removed. This value is used if the Probe Count was not defined on the interface.
- Default Probe Interval – The default interval (in seconds) between the probes sent by the device. This value is used if the Probe Interval was not defined on the interface.
- Probe Delay Interval – the time (in seconds) to wait after a link moves to the up state before sending a probe. This setting is useful in case sending the probe too soon will affect the connected station DHCP process.
- Auto Source IP Address Value – the IP address to use as the source IP address for probes that are sent by VLAN interfaces that are not configured with an IP address.
- Auto Source IP Wildcard Mask (available for configuration only if the Auto Source IP Address Value is configured) – the mask is to apply to the Auto Source IP Address. Only the host portion of the Source IP Address will be used for the probe source address.
- Total number of interfaces enabled (read-only) – indicates that the number of interfaces IP device trackings is enabled on.

Step 3 Click **Apply** to apply the settings.

Explanation for the fields in the IP Device Tracking Settings Table:

- Port – device port
- Administrative Status – the state IP Device Tracking setting on the interface. Supported values:
  - Enable – IP device tracking was enabled on the interface by the user.
  - Disable – IP device tracking was disabled on the interface by the user.
  - Auto (default state) – IP device Tracking is active on the interface if the interface 802.1x Administrative Port Control setting is set to auto.
- Operational Status – the operational status of the feature on the interface.
- Maximum Hosts – the maximum number of hosts that can be added to the IP device tracking table on this interface. A value of 0 indicates that the feature is disabled on the interface.
- Application – will indicate if 802.1x is enabled on the interface. This activates IP device tracking on the interface when the Administrative status is auto.
- Probe Count – the number of probes sent on this interface before a host entry is removed from the IP device tracking table. If the (Default) indication is also present it means that the default global probe count value applied the probe count value.
- Probe Interval – The default interval (in seconds) between the probes sent on this interface. If the (Default) indication is also present it means that the probe Interval value was applied by the default global probe Interval value.

Step 4 To edit the settings of an interface, select the interface row in the table and click the **Edit**.

Step 5 Next, configure the following:

- Interface –Select the interface from the drop-down.
- Port – Select the port from the drop-down.
- IP Device Tracking Operational Status – displays the status of the IP device tracking feature on this interface (read-only field).
- IP Device Tracking Administrative Status – set the administrative status on the interface:
  - Auto (default state) – IP device Tracking is active on the interface only if the 802.1x Administrative Port Control setting is set to auto.
  - Disable – IP device tracking is disabled on the interface.
  - Enable – IP device tracking is enabled on the interface.
- Maximum Hosts – maximum number of hosts that can be added to the IP Device tracking table. This setting is mandatory if the IP Device Tracking Administrative Status is set to enable.
- Probe Count – the number of probes sent on this interface before a host entry is removed from the IP device tracking table. If the (Default) indication is also present it means that the default global probe count value applied the probe count value.

- Probe Interval – The default interval (in seconds) between the probes sent on this interface. If the (Default) indication is also present it means that the probe Interval value was applied by the default global probe Interval value.