

# Administration

This chapter contains the following sections:


- System Settings, on page 1
- IOS Configuration Conversion, on page 2
- Console Settings , on page 2
- Bluetooth Settings, on page 3
- User Accounts, on page 5
- Idle Session Timeout, on page 6
- Time Settings, on page 7
- System Log, on page 14
- File Management, on page 18
- Cisco Business Dashboard Settings, on page 27
- Plug-n-Play (PNP), on page 30
- Reboot, on page 36
- Discovery - Bonjour, on page 37
- Discovery - LLDP, on page 38
- Discovery - CDP, on page 53
- Locate Device, on page 60
- Ping, on page 61
- Traceroute, on page 62


# System Settings

The system setting page allows you customize the settings on your switch. You can configure the following:

**Procedure**

**Step 1** Click **Administration** > **System Settings**.

**Step 2** View or modify the system settings.

- System Description—Displays a description of the device.
- System Location—Enter the physical location of the device.

- System Contact—Enter the name of a contact person.
- Host Name—Select the host name of this device. This is used in the prompt of CLI commands:
  - Use Default—The default hostname (System Name) of these switches is: switch123456, where 123456 represents the last three bytes of the device MAC address in hex format.
  - User Defined—Enter the hostname. Use only letters, digits, and hyphens. Host names can't begin or end with a hyphen. No other symbols, punctuation characters, or blank spaces are permitted (as specified in RFC1033, 1034, 1035).

**Custom Banner Settings**

The following banners can be set:

- Login Banner—Enter text to display on the Login page before login. Click **Preview** to view the results.
- Welcome Banner—Enter text to display on the Login page after login. Click **Preview** to view the results.

**Note**
When you define a login banner from the web-based configuration utility, it also activates the banner for the CLI interfaces (Console, Telnet, and SSH).

The banner can contain up to 1000 characters. After 510 characters, press <Enter> to continue.

**Step 3** Click **Apply** to save the new settings.

# IOS Configuration Conversion

The IoS conversion tool converts a Catalyst 1000 configuration file to a Catalyst 1200/ Catalyst 1300 configuration file. This will allow easy transition of a network from Catalyst 1000 devices to Catalyst 1200/1300 devices.

To start the configuration process, complete the following:

1. Click **Administration > IoS Configuration Conversion**.
2. Click **Go**. You will be redirected to https://cisco.com/go/iosconversiontool.

   Log in and upload the traditional catalyst switch configuration file and get it converted to a Catalyst 1200/1300 configuration.

# Console Settings

**Note** The Console Setting is only available in the Advanced Mode view.

The console port speed can be set to one of the following speeds: 9600, 19200, 38400, 57600, and 115200 or to Auto Detection. If Auto Detection is selected, the device detects console speed automatically. When Auto Detection is not enabled, the console port speed is automatically set to the last speed that was set manually at

(115,200 by default). When Auto Detection is enabled but the console baud-rate has not yet been discovered, the system uses speed 115,200 for displaying text (for example, the boot-up information). After Auto Detection is enabled in the Console Settings page, it can be activated by connecting the console to the device and pressing the Enter key twice. The device detects the baud rate automatically.

To enable Auto Detection or to manually set the baud rate of the console, follow these steps:

**Procedure**

**Step 1** Click **Administration** > **Console Settings**.

**Step 2** Select one of the following options in the Console Port Baud Rate field:

- Auto Detection—The console baud rate is detected automatically.
- Static—Select one of the available speeds.

**Step 3** Click **Apply**.

# Bluetooth Settings

Bluetooth allows devices to wirelessly connect and communicate with each other over short distances. It is a convenient, versatile, and reliable technology that is used in many applications.

Support of Bluetooth is achieved by connecting a Bluetooth (BT) dongle, to the device USB port. The device will automatically detect the insertion of a supported BT dongle into device's USB port, and provide Bluetooth support, which enables BT operation. The Bluetooth interface in the device management interface allows the user to apply relevant Bluetooth settings. In the CLI and text configuration file, the Bluetooth interface is known as "interface bluetooth 0". Even if a BT dongle is not inserted into the USB port, the BT interface allows configuration.

List of supported dongles:

- BTD-400 Bluetooth 4.0 Adapter by Kinivo
- Bluetooth 4.0 USB Adapter by Asus
- Bluetooth 4.0 USB Adapter by Insignia
- Philips 4.0 Bluetooth adapter
- Lenovo LX1815 Bluetooth 5.0 USB adapter
- Lenovo LX1812 Bluetooth 4.0 USB adapter

In a stack, BT dongle detection and operation will be supported only on the stack Active unit. The device supports detection of a single USB device into USB port, meaning device does not support multiple USB dongles or USB dongle + memory stick on the same USB interface.

Notification syslog messages will indicate successful detection and removal of BT dongle, as follows:

- Dongle insertion – "Bluetooth Dongle inserted into USB port"

• Dongle removal – “Bluetooth Dongle removed from USB port”

To configure the bluetooth settings, complete the following steps:

### Procedure

**Step 1** Click **Administration** > **Bluetooth Settings**.

**Step 2** Configure the following settings:

| | |
|---|---|
| Bluetooth Service | Check **Enable** to enable bluetooth service on the device. Default is enable. |
| PIN | Select from the following:<br>• Encrypted - Enter an encrypted PIN<br>• Plaintext - Enter a plaintext PIN (4 digits)<br>Default PIN is 9999 |
| Bluetooth Device Name | The string by which the device advertises itself over bluetooth. Select from the following:<br>• Switch Host Name (Default)<br>• User Defined - Enter a user defined name (Up to 20 characters) |
| BT Interface Description | Enter a description for the bluetooth interface. (0 - 64 characters) |
| BT IP Interface | The IP interface used to manage the device over the bluetooth interface. Select from the following:<br>• None - an IP address is not configured on the bluetooth interface.<br>• User Defined - configure an IP address and mask on the Bluetooth interface.<br>**Note**<br>Both BT IP address and BT IP Mask fields are associated with the previous item of BT IP interface and are active only if the user selects User Defined for BT IP Interface. |
| BT IP Address | Enter the bluetooth interface IP address. |
| BT IP Mask | The IP Mask/Prefix length of the IP address. This control is only enabled if the IP Interface is user defined. Select from the following:<br>• Network Mask<br>• Prefix Length |
| Dongle Present | Will display if a dongle is present. |

| | |
|---|---|
| State | Displays the state of the bluetooth connection. Available states are:<br>• Not Ready (dongle is not inserted)<br>• Discoverable (dongle is inserted and discoverable)<br>• Connected (connected to bluetooth partner)<br>• Disabled (bluetooth interface was disabled) |
| Connected Device Name | The display name of the connected Bluetooth device. This field appears only if a Bluetooth connection was established between the Switch and a remote Bluetooth device. |

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

**Step 4** Click **Display Sensitive Data as Plaintext** to display the sensitive data as plain text.

# User Accounts

The User Accounts page enables entering additional users that are permitted to access to the device (read-only or read-write) or changing the passwords of existing users. A user accessing the device for the first time uses the cisco/cisco username and password. After providing the default credentials, you're prompted to replace the default level 15 username and password, and you must provide a new username and password. The new password must comply with the password complexity rules.

To add a new user, follow these steps:

### Procedure

**Step 1** Click **Administration** > **User Accounts**.

**Step 2** In the Password Recovery Service, check **Enable** to enable password recovery.

**Step 3** Click **Add** to add a new user or click **Edit** to modify a user and/or the password.

**Step 4** Enter the parameters.

- User Name—Enter a new username from 0 through 20 characters. UTF-8 characters aren't permitted.
- Current Password — Enter the current password. (This field will only appear in Edit mode).
- Suggest Password— Click to auto generate a password. Next, click **Copy to Clipboard** to copy the password and click **Yes** if you would like to use the password for this account.
- Password—Enter a password (UTF-8 characters aren't permitted).

**Note**
Please refer to the password complexity rule section in Login Settings before creating a password.

**Note**
The password entered by the user is compared to a list of well known common passwords. If the password contains words from this list, the password will be rejected and a new one will need to be entered.

- Confirm Password—Enter the password again.
- Password Strength Meter—Displays the strength of password.
- User Level—Select the privilege level of the user.
  - Read-Only CLI Access (1)—User can't access the GUI and can only access CLI commands that don't change the device configuration.
  - Read/Limited Write CLI Access (7)—User can't access the GUI and can only access some CLI commands that change the device configuration. See the *CLI Reference Guide* for more information.
  - Read/Write Management Access (15)—User can access the GUI and can configure the device.

**Step 5** Click **Apply**. The user is added to the Running Configuration file of the device.

**Note**
The password is stored in the configuration files as a non-recoverable hash using Password Based Key Derivation Function 2 (PBKDF2) with Secure Hash Algorithm, and SHA-512 as the hashing algorithm.

# Idle Session Timeout

The Idle Session Timeout configures the time intervals that the management sessions can remain idle before they timeout.

To set the idle session timeout for various types of sessions, complete these steps:

**Procedure**

**Step 1** Click **Administration** > **Idle Session Timeout**.

**Step 2** Select the timeout for each type of session from the list.

- HTTP Session Timeout
- HTTPS Session Timeout
- Console Session Timeout
- Telnet Session Timeout
- SSH Session Timeout

The default timeout value is 10 minutes. You must log in again to reestablish one of the chosen sessions.

**Step 3** Click **Apply** to set the configuration settings on the device.

# Time Settings

**Note** This setting is only available in the Advanced Mode view.

Synchronized system clocks provide a frame of reference between all devices on the network. Network time synchronization is critical because every aspect of managing, securing, planning, and debugging a network involves determining when events occur. Without synchronized clocks, accurately correlating log files between devices when tracking security breaches or network usage is impossible. Synchronized time also reduces confusion in shared file systems, as it is important for the modification times to be consistent, regardless of the machine on which the file systems reside. For these reasons, it is important that the time configured on all of the devices on the network is accurate.

### Real Time Clock

Some devices have an internal self-sufficient Real Time Clock (RTC) component that keeps time even when the device is shut down and not connected to a power source. This internal clock is initialized during manufacturing and can be updated by the time features of the device when the software clock is set. When a device with a functional RTC component starts up, the system clock is set to the time and date of the RTC. The RTC component is updated whenever the system clock is changed - either dynamically by the Simple Network Time Protocol (SNTP), or manually.

**Note** The device supports SNTP, and when enabled, the device dynamically synchronizes the device time with time from an SNTP server. The device operates only as an SNTP client, and cannot provide time services to other devices.

## System Time

Use the System Time page to select the system time source. If the source is manual, you can enter the time here.

**Caution** If the system time is set manually and the device is rebooted, the manual time settings must be reentered.

To define system time, complete these steps:

### Procedure

**Step 1** Click **Administration** > **Time Settings** > **System Time**.

The following fields are displayed:

- Actual Time (From SNTP Server)— Actual system time on the device.

- Last Synchronized Server—Address, stratum and type of the SNTP server from which system time was last taken.

**Step 2** Enter the following parameters:

- Clock Source Settings—Select the source used to set the system clock.
  - Main Clock Source (SNTP Servers)—If this is enabled, the system time is obtained from an SNTP server. To use this feature, you must also configure a connection to an SNTP server in the SNTP Multicast/Anycast, on page 11.
  - Alternate Clock Source (PC via active HTTP/HTTPS sessions)— Check **Enable** to enable the date and time from the configuring computer using the HTTP protocol.

    **Note**
    The Clock Source Setting must be set to either of the above for RIP MD5 authentication to work.

- Manual Settings—Set the date and time manually. The local time is used when there's no alternate source of time, such as an SNTP server:
  - Date—Enter the system date.
  - Local Time—Enter the system time.

- Time Zone Settings—The local time is used via the DHCP server or Time Zone offset.
  - Get Time Zone from DHCP—Select to enable dynamic configuration of the time zone and the DST from the DHCP server. Whether one or both of these parameters can be configured depends on the information found in the DHCP packet. If this option is enabled, DHCP client must be enabled on the device.
  - Time Zone from DHCP—Displays the acronym of the time zone configured from the DHCP server. This acronym appears in the Actual Time field.
  - Time Zone Offset—Select the difference in hours between Greenwich Mean Time (GMT) and the local time. For example, the Time Zone Offset for Paris is GMT +1, while the Time Zone Offset for New York is GMT – 5.
  - Time Zone Acronym—Enter a name that represents this time zone. This acronym appears in the Actual Time field.

- Daylight Savings Settings—Select how DST is defined:
  - Daylight Savings—Select to enable Daylight Saving Time.
  - Time Set Offset—Enter the number of minutes offset from GMT ranging 1—1440. The default is 60.
  - Daylight Savings Type—Click one of the following:

    USA—DST is set according to the dates used in the USA.

    European—DST is set according to the dates used by the European Union and other countries that use this standard.

    By dates—DST is set manually, typically for a country other than the USA or a European country. Enter the parameters described below.

    Recurring—DST occurs on the same date every year.

    Selecting By Dates allows customization of the start and stop of DST:

- From—Day and time that DST starts.
- To—Day and time that DST ends.

**Step 3** Selecting Recurring allows different customization of the start and stop of DST:

- From—Date when DST begins each year.
  - Day—Day of the week on which DST begins every year.
  - Week—Week within the month from which DST begins every year.
  - Month—Month of the year in which DST begins every year.
  - Time—The time at which DST begins every year.
- To—Date when DST ends each year. For example, DST ends locally every fourth Friday in October at 5:00 a.m.. The parameters are:
  - Day—Day of the week on which DST ends every year.
  - Week—Week within the month from which DST ends every year.
  - Month—Month of the year in which DST ends every year.
  - Time—The time at which DST ends every year.

**Step 4** Click **Apply**. The system time values are written to the Running Configuration file.

# SNTP Unicast

SNTP synchronizes a computer's system time with a server that has already been synchronized by a source such as a satellite receiver or modem. SNTP supports unicast, multicast and anycast operating modes. In unicast mode, the client sends a request to a dedicated server by referencing its unicast address. Up to 16 Unicast SNTP servers can be configured.

**Note** The Main Clock Source (SNTP Servers) System Time, on page 7 must be enable for SNTP Client Unicast to operate.

To add a Unicast SNTP server, follow these steps:

### Procedure

**Step 1** Click **Administration** > **Time Settings** > **SNTP Unicast**.

**Step 2** Configure the following fields:

| | |
|---|---|
| SNTP Client Unicast | Select **Enable** to enable the device to use SNTP-predefined Unicast clients with Unicast SNTP servers. |

| | |
|---|---|
| IPv4 Source Interface | Select the IPv4 interface from the drop-down list used for communication with the SNTP server. |
| IPv6 Source Interface | Select the IPv6 interface from the drop-down list used for communication with the SNTP server.<br>**Note**<br>If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface. |

This page displays the following information for each Unicast SNTP server:

- SNTP Server—SNTP server IP address. The preferred server, or hostname, is chosen according to its stratum level.
- Poll Interval—Displays whether polling is enabled or disabled.
- Authentication Key ID—Key Identification used to communicate between the SNTP server and device.
- Stratum Level—Distance from the reference clock expressed as a numerical value. An SNTP server cannot be the primary server (stratum level 1) unless polling interval is enabled.
- Status—SNTP server status. The possible values are:
  - Up—SNTP server is currently operating normally
  - Down—SNTP server is currently not available.
  - Unknown—SNTP server status is unknown.
  - In Process—Connection to SNTP server currently in process.
- Last Response—Last date and time a response was received from this SNTP server.
- Offset—Estimated offset of the server's clock relative to the local clock, in milliseconds. The host determines the value of this offset using the algorithm described in RFC 2030.
- Delay—Estimated round-trip delay of the server's clock relative to the local clock over the network path between them, in milliseconds. The host determines the value of this delay using the algorithm described in RFC 2030.
- Source—How the SNTP server was defined, for example: manually or from DHCPv6 server.
- Interface—Interface on which packets are received.

**Step 3** Click **Add** to add a Unicast SNTP server.

**Note**
To remove all user-defined SNTP servers, click **Restore Default Servers**.

**Step 4** Enter the following parameters:

| | |
|---|---|
| Server Definition | Select the SNTP server to be identified by its IP address or by name from the list. |
| IP Version | Select the version of the IP address: Version 6 or Version 4. |

| | |
|---|---|
| IPv6 Address Type | Select the IPv6 address type (if IPv6 is used). The options are:<br>• 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.<br>• Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks. |
| Link Local Interface | Select the link local interface (if IPv6 Address Type Link Local is selected) from the list. |
| SNTP Server IP Address/Name | Enter the SNTP server IP address or name. The format depends on which address type was selected. |
| Poll Interval | Select to enable polling of the SNTP server for system time information. All NTP servers that are registered for polling are polled, and the clock is selected from the server with the lowest stratum level that is reachable. The server with the lowest stratum is considered to be the primary server. The server with the next lowest stratum is a secondary server, and so forth. If the primary server is down, the device polls all servers with the polling setting enabled, and selects a new primary server with the lowest stratum. |
| Authentication | Select the check box to enable authentication. |
| Authentication Key ID | If authentication is enabled, select the value of the key ID. |

**Step 5** Click **Apply**. The STNP server is added, and you are returned to the main page.

# SNTP Multicast/Anycast

**Note** This setting is only available in the Advanced Mode view.

**Note** The Main Clock Source (SNTP Servers) System Time, on page 7 must be enable for SNTP Client Multicast/Anycast to operate.

To enable receiving SNTP packets from all servers on the subnet and/or to enable transmitting time requests to SNTP servers, follow these steps:

**Procedure**

**Step 1** Click **Administration** > **Time Settings** > **SNTP Multicast/Anycast**.

Select from the following options to enable:

| Option | Description |
|---|---|
| SNTP IPv4 Multicast Client Mode (Client Broadcast Reception) | Check **Enable** to receive system time IPv4 Multicast transmissions from any SNTP server on the subnet. |
| SNTP IPv6 Multicast Client Mode (Client Broadcast Reception) | Check **Enable** to receive system time IPv6 Multicast transmissions from any SNTP server on the subnet. |
| SNTP IPv4 Anycast Client Mode (Client Broadcast Transmission) | Check **Enable** to transmit SNTP IPv4 synchronization packets requesting system time information. The packets are transmitted to all SNTP servers on the subnet. |
| SNTP IPv6 Anycast Client Mode (Client Broadcast Transmission) | Check **Enable** to transmit SNTP IPv6 synchronization packets requesting system time information. The packets are transmitted to all SNTP servers on the subnet. |

**Step 2** Click **Add** to select the interface for SNTP.

Select the interface (Port, LAG or VLAN) and configure by selecting an option from the drop-down menu.

**Step 3** Click **Apply** to save the settings to the Running Configuration file.

# SNTP Authentication

**Note** This setting is only available in the Advanced Mode view.

SNTP clients can authenticate responses by using HMAC-MD5. An SNTP server is associated with a key. This is used as input together with the response itself to the MD5 function; the result of the MD5 is also included in the response packet. The SNTP Authentication page enables configuration of the authentication keys that are used when communicating with an SNTP server.

The authentication key is created on the SNTP server in a separate process that depends on the SNTP server type. Consult with the SNTP server system administrator for more information.

### Procedure

**Step 1** Click **Administration** > **Time Settings** > **SNTP Authentication**.

**Step 2** Check **Enable** to enable SNTP authentication of an SNTP session between the device and an SNTP server.

**Step 3** Click **Apply** to update the device.

**Step 4** Click **Add.**

**Step 5** Enter the following parameters:

- Authentication Key ID—Enter the number used to identify this SNTP authentication key internally.
- Authentication Key—Select from the following options:
  - User Defined (Encrypted)—Enter the key used for authentication in encrypted format. The SNTP server must send this key for the device to synchronize to it.

- User Defined (Plaintext)—Enter the key used for authentication (up to eight characters) in plaintext format. The SNTP server must send this key for the device to synchronize to it.

- Authentication Method—select the method to use for the authentication with the server. The supported methods are: MD5; SHA1; SHA2-256 and HMAC-SHA2-256.
- Trusted Key—Check to enable the device to receive synchronization information only from a SNTP server by using this authentication key.

**Step 6** Click **Apply**. The SNTP Authentication parameters are written to the Running Configuration file.

**Step 7** To delete an SNTP Authentication Key, check the the desired Authentication Key ID and click the **Delete** icon.

**Step 8** To display sensitive data in plaintext form on the page, click **Display Sensitive Data As Plaintext**.

# Time Range

Time ranges can be defined and associated with the following types of commands, so that they are applied only during that time range:

- Port Stat
- Time-Based PoE

There are two types of time ranges:

- Absolute—This type of time range begins on a specific date or immediately and ends on a specific date or extends infinitely. It is created in the Time Range pages. A periodic element can be added to it.
- Periodic—This type of time range contains a time range element that is added to an absolute range, and begins and ends on a periodic basis. It is defined in the Periodic Range pages.

If a time range includes both absolute and periodic ranges, the process associated with it is activated only if both absolute start time and the periodic time range have been reached. The process is deactivated when either of the time ranges are reached. The device supports a maximum of 20 absolute time ranges.

To ensure that the time range entries take effect at the desired times, the system time must be set.The time-range feature can be used for the following:

- Limit access of computers to the network during business hours (for example), after which the network ports are locked, and access to the rest of the network is blocked (see Configuring Ports and Configuring LAG Settings)
- Limit PoE operation to a specified period.

  Add these descriptions for time range

### Procedure

**Step 1** Click **Administration** > **Time Settings** > **Time Range**.

**Step 2** In the Time Range Table, click **Add** to add a new time range or **Edit** or **Delete** to edit or delete an existing one.

**Step 3** To add a new time range, click **Add** and configure the following:

- Time Range Name—Enter a name for your time range
- Absolute Starting Time—Select Immediate or enter a date and time.
- Absolute Ending Time—Select Infinite or enter a date and time

**Step 4** Click **Apply** to apply the new time range settings.

# Recurring Range

**Note** This setting is only available in the Advanced Mode view.

A recurring time element can be added to an absolute time range. This limits the operation to certain time periods within the absolute range.

To add a recurring time range element to an absolute time range:

**Procedure**

**Step 1** Click **Administration** > **Time Settings** > **Recurring Range**.

The existing recurring time ranges are displayed (filtered per a specific, absolute time range.)

**Step 2** Select the absolute time range to which to add the recurring range.

**Step 3** To add a new recurring time range, click **Add**.

**Step 4** Enter the following fields:

- Recurring Starting Time—Enter the day of the week, and time that the Time Range begins.
- Recurring Ending Time—Enter the day of the week, and time that the Time Range ends.

**Step 5** Click **Apply.**

# System Log

This section describes the system logging, which enables the device to generate multiple independent logs. Each log is a set of messages describing system events.

The device generates the following local logs:

- Log sent to the console interface.
- Log written into a cyclical list of logged events in the RAM and erased when the device reboots.
- Log written to a cyclical log-file saved to the Flash memory and persists across reboots.

In addition, you can send messages to remote SYSLOG servers in the form of SNMP traps and SYSLOG messages.

# Log Settings

You can select the events to be logged by severity level. Each log message has a severity level marked with the first letter of the severity level concatenated with a dash (-) on each side (except for Emergency that is indicated by the letter F). For example, the log message "%INIT-I-InitCompleted: … " has a severity level of I, meaning Informational.

The event severity levels are listed from the highest severity to the lowest severity, as follows:

- Emergency—System is not usable.
- Alert—Action is needed.
- Critical—System is in a critical condition.
- Error—System is in error condition.
- Warning—System warning has occurred.
- Notice—System is functioning properly, but a system notice has occurred.
- Informational—Device information.
- Debug—Detailed information about an event.

You can select different severity levels for RAM and Flash logs. These logs are displayed in the RAM Memory and Flash Memory, respectively.

Selecting a severity level to be stored in a log causes all of the higher severity events to be automatically stored in the log. Lower severity events are not stored in the log. For example, if Warning is selected, all severity levels that are Warning and higher are stored in the log (Emergency, Alert, Critical, Error, and Warning). No events with severity level below Warning are stored (Notice, Informational, and Debug).

To set global log parameters, complete the following steps:

### Procedure

**Step 1** Click **Administration** > **System Log** > **Log Settings**.

**Step 2** Enter the parameters.

| | |
|---|---|
| Logging | Select to enable message logging. |
| Syslog Aggregator | Select to enable the aggregation of SYSLOG messages and traps. If enabled, identical and contiguous SYSLOG messages and traps are aggregated over the specified Max. Aggregation Time and sent in a single message. The aggregated messages are sent in the order of their arrival. Each message states the number of times it was aggregated. |
| Max. Aggregation Time | Enter the interval of time that SYSLOG messages are aggregated. |
| Enable Flash memory logging threshold | Check to enable. |

| | |
|---|---|
| Flash memory logging thereshold | Enter the percentage (Range: 1 - 99) |
| Originator Identifier | Enables adding an origin identifier to SYSLOG messages. The options are:<br>• None—Do not include the origin identifier in SYSLOG messages.<br>• Hostname—Include the system host name in SYSLOG messages.<br>• IPv4 Address—Include the IPv4 address of the sending interface in SYSLOG messages.<br>• IPv6 Address—Include the IPv6 address of the sending interface in SYSLOG messages.<br>• User Defined—Enter a description to be included in SYSLOG messages. |
| Log Timestamp Timezone | Defines the timezone of the timestamp. Timezone can be set to UTC or local. The default timezone setting is local. Select the timezone that will be used for the time presented in the timestamp:<br>• Local Time<br>• UTC |
| Include Milliseconds | Defines if the timestamp should included milliseconds. By default, the timestamp does not include milliseconds. Select if the timestamp will include. |
| Show Timezone | Defines if the timezone should be displayed as part of the timestamp. By default timezones are not included in the timestamp. Select if the timestamp will include the acronym of the timezone. |
| RAM Memory Logging | Select the severity levels of the messages to be logged to the RAM. |
| Flash Memory Logging | Select the severity levels of the messages to be logged to the Flash memory. |

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

# Remote Log Servers

The Remote Log Servers page enables defining remote SYSLOG servers to which log messages are sent. For each server, you can configure the severity of the messages that it receives.

To define SYSLOG servers, follow these steps:

**Procedure**

**Step 1** Click **Administration** > **System Log** > **Remote Log Servers**.

**Step 2**
**Note**
This setting is only available in the Advanced Mode view.

Enter the following fields:

- IPv4 Source Interface—Select the source interface whose IPv4 address will be used as the source IPv4 address of SYSLOG messages sent to SYSLOG servers.
- IPv6 Source Interface—Select the source interface whose IPv6 address will be used as the source IPv6 address of SYSLOG messages sent to SYSLOG servers.

**Note**
If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

Information is described for each previously configured log server. The fields are described below in the Add page.

**Step 3** Click **Add**.

**Step 4** Enter the parameters.

| | |
|---|---|
| Server Definition | Select whether to identify the remote log server by IP address or name. |
| IP Version | Select the supported IP format. |
| IPv6 Address Type | Select the IPv6 address type (if IPv6 is used). The options are:<br>• Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80::/10, 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.<br>• Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks. |
| Link Local Interface | Select the link local interface (if IPv6 Address Type Link Local is selected) from the list. |
| Log Server IP Address/Name | Enter the IP address or domain name of the log server. |
| Protocol | Select the protocol to use for sending syslog messages. The supported values are UDP or TCP. |
| UDP/TCP Port | Enter the UDP or TCP port to which the log messages are sent. |
| Facility | Select a facility value from which system logs are sent to the remote server. Only one facility value can be assigned to a server. If a second facility code is assigned, the first facility value is overridden. |
| Description | Enter a server description. |
| Minimum Severity | Select the minimum level of system log messages to be sent to the server. |

**Step 5** Click **Apply.** The Add Remote Log Server page closes, the SYSLOG server is added, and the Running Configuration file is updated.

# File Management

A File Management System is an application that is used to store, arrange and access the files that are on your device. The system files are files that contain information, such as: configuration information or firmware images. Generally, every file under the flash://system/ folder is a system file. Various actions can be performed with these files, such as: selecting the firmware file from which the device boots, modifying various types of configuration files internally on the device, or copying files to or from an external device, such as an external server.

The following are some of the types of files are found on the device:

- Running Configuration—Contains the parameters currently being used by the device to operate. This file is modified when you change parameter values on the device. If the device is rebooted, the Running Configuration is lost. To preserve any changes you made to the device, you must save the Running Configuration to the Startup Configuration, or another file type.
- Startup Configuration—The parameter values that saved by copying another configuration (usually the Running Configuration) to the Startup Configuration. The Startup Configuration is retained in Flash and is preserved when the device is rebooted. At this time, the Startup Configuration is copied to RAM and identified as the Running Configuration.
- Mirror Configuration—A copy of the Startup Configuration, created by the device when the following conditions exist:
  - The device has been operating continuously for 24 hours.
  - No configuration changes have been made to the Running Configuration in the previous 24 hours.
  - The Startup Configuration is identical to the Running Configuration.

  Only the system can copy the Startup Configuration to the Mirror Configuration. However, you can copy from the Mirror Configuration to other file types or to another device.
- Backup Files—Manual copies of a files used for protection against system shutdown or for the maintenance of a specific operating state. For instance, you can copy the Mirror Configuration, Startup Configuration, or Running Configuration to a Backup file. The Backup exists in Flash or on a PC or USB drive and is preserved if the device is rebooted.
- Firmware—The program that controls the operations and functionality of the device. More commonly referred to as the image.
- Language File—The dictionary that enables the web-based configuration utility windows to be displayed in the selected language.
- Logging File—SYSLOG messages stored in Flash memory.

# Firmware Operations

The Firmware Operations page can be used to:

- Update or backup the firmware image
- Swap the active image.

The software images of the units in a stack must be identical to ensure proper stack operations. Stack units can be upgraded in any one of the following ways.

### Procedure

**Step 1** Click **Administration** > **File Management** > **Firmware Operations**.

The following fields are displayed:

- Active Firmware File—Displays the current, active firmware file.
- Active Firmware Version—Displays the version of the current, active firmware file.

**Step 2** Select the **Operation Type** from the following options:

- Update Firmware
- Backup Firmware
- Swap Image

**Step 3** Select the **Copy Method** from the following options:

| | |
|---|---|
| HTTP/HTTPS | For HTTP/HTTPS, enter the file name in the File Name field, or browse to locate and select the file. |
| USB | For USB, enter the file name in the File Name field, or browse to locate and select the file. |
| TFTP | For TFTP, proceed with the TFTP Instructions below. |
| SCP (File transfer via SSH) | For SCP, proceed with the SCP Instructions below. |

**TFTP Instructions**

**Note**
This setting is only available in the Advanced Mode view.

Configure the following if you selected the TFTP as your copy method for the firmware operations.

| | |
|---|---|
| Server Definition | Select from the following options:<br>• By IP Address<br>• By Name |
| IP Version | Select from the following options:<br>• IP Version 6<br>• IP Version 4 |

| | |
|---|---|
| IPv6 Address Type | Select from the following options:<br>• Link Local—A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network.<br>• Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks. |
| Link Local Interface | If for the IPv6 address type, you selected Link Local, select the interface from the drop down list. |
| Server IP Address/Name | Enter the server IP address/name. |
| Source (Appears when in updating firmware) | Enter the name of the source (0- 62 characters used) |
| Destination (Appears when in backing up firmware) | Enter the destination (0 - 62 characters used) |

**SCP Instructions**

**Note**
This setting is only available in the Advanced Mode view.

Configure the following if you selected the SCP as your copy method for the firmware operations.

| | |
|---|---|
| Remote SSH Server Authentication | To enable SSH server authentication (which is disabled by default), click **Edit** . |
| SSH Client Authentication | Select from the following:<br>• Use SSH Client System Credentials.<br>• Use SSH Client One-Time Credentials: |
| Username | Enter the username if using the SSH Client One-Time Credentials option. |
| Password | Enter the password if using the SSH Client One-Time Credentials option. |
| Server Definition | Select from the following options:<br>• By IP Address<br>• By Name |
| IP Version | Select from the following options:<br>• Version 6<br>• Version 4 |

| | |
|---|---|
| IPv6 Address Type | Select from the following options:<br>• Link Local—A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network.<br>• Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks. |
| Link Local Interface | If for the IPv6 address type, you selected Link Local, select the interface from the drop down list. |
| Server IP Address/Name | Enter the server IP address/name. |
| Source (Appears when in updating firmware) | Enter the name of the source (0 - 62 characters used) |
| Destination (Appears when in backing up firmware) | Enter the destination (0 - 62 characters used) |

**Step 4** Click **Apply** to save your settings.

# File Operations

### Procedure

**Step 1** Click **Administration** > **File Management** > **File Operations**.

**Step 2** Select the Operation Type from the following options:

- Update File
- Backup File
- Duplicate

**Step 3** Select the Destination or Source File Type from the following options:

- Running Configuration
- Startup Configuration
- Mirror Configuration
- Logging File
- Language File
- Dashboard Info File

**Step 4** Select the Copy Method from the following options:

| | |
|---|---|
| HTTP/HTTPS | For HTTP/HTTPS, enter the file name in the File Name field, or browse to locate and select the file. |
| USB | For USB, enter the file name in the File Name field, or browse to locate and select the file. |
| Internal Flash | For Internal File, enter the file name in the File name field or click on File Directory to browse and to locate. Sensitive Data Handling - Select the method in which the data should be handled. This applies only for file backup.<br>• Exclude—to exclude sensitive data<br>• Encrypt—to encrypt sensitive data<br>• Plaintext—to display sensitive data in plaintext. |
| TFTP | For TFTP, proceed with the TFTP Instructions below. |
| SCP (File transfer via SSH) | For SCP, proceed with the SCP Instructions below. |

**TFTP Instructions**

Configure the following if you selected the TFTP as your update or backup method for the file operations.

| | |
|---|---|
| Server Definition | Select from the following options:<br>• By IP Address<br>• By Name |
| IP Version | Select from the following options:<br>• IP Version 6<br>• IP Version 4 |
| IPv6 Address Type | Select from the following options:<br>• Link Local—A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network.<br>• Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks. |
| Link Local Interface | If for the IPv6 address type, you selected Link Local, select the interface from the drop down list. |
| Server IP Address/Name | Enter the server IP address/name. |
| Source | Enter the name of the source (0 - 62 characters used) |

| | |
|---|---|
| Sensitive Data Handling | **Note**<br>This option only appears when in Backup file mode for SCP or TFTP.<br><br>Select how sensitive data should be included in the backup file from one of the following options:<br>• Exclude—Do not include sensitive data in the backup.<br>• Encrypt—Include sensitive data in the backup in its encrypted form.<br>• Plaintext—Include sensitive data in the backup in its plaintext form. |

**SCP Instructions**

Configure the following if you selected the SCP as your copy method for the file operations.

| | |
|---|---|
| Remote SSH Server Authentication | To enable SSH server authentication (which is disabled by default), click **Edit** . |
| SSH Client Authentication | Select from the following:<br>• Use SSH Client System Credentials:<br>• Use SSH Client One-Time Credentials: |
| Username | Enter the username if using the SSH Client One-Time Credentials option. |
| Password | Enter the password if using the SSH Client One-Time Credentials option. |
| Server Definition | Select from the following options:<br>• By IP Address<br>• By Name |
| IP Version | Select from the following options:<br>• IP Version 6<br>• IP Version 4 |
| IPv6 Address Type | Select from the following options:<br>• Link Local—A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network.<br>• Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks. |
| Link Local Interface | If for the IPv6 address type, you selected Link Local, select the interface from the drop down list. |
| Server IP Address/Name | Enter the server IP address/name. |
| Source | Enter the name of the source (0 - 62 characters used) |

**Step 5** If selecting HTTP/HTTPS as your copy method, in the File name section, click the **Browse** button to locate and select the file.

**Step 6** Click **Apply** to save the settings.

## Back Up the Configuration

Backing up configuration files is essential in case of product failure to minimize downtime. Additionally, It is recommended backing up a good known working configuration file prior to testing a new configuration on your production or testing equipment. After verifying the configuration changes are working as expected, make sure to apply the changes and create a new backup configuration file.

To back up and restore the configuration on a the switch, you can use the device's web-based graphical user interface (GUI). Here are the steps to back up and restore the switch configuration:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Log in to the switch's web-based GUI. | |
| **Step 2** | Navigate to **Administration > File Management > File Operations**. | |
| **Step 3** | Under Operation Type, select **Backup File**. | |
| **Step 4** | Next, in the Source File Type, select **Running Configuration**. | |
| **Step 5** | For the Copy Method, select from one of the following options: | • HTTP/HTTPS<br>• USB<br>• Internal Flash |
| **Step 6** | Next, select the Sensitive Data Handling option from the following: | • Exclude<br>• Encrypt<br>• Plaintext |
| **Step 7** | Click **Apply**. | |

## Restore the Configuration

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Log in to the switch's web-based GUI. | |
| **Step 2** | Navigate to **Administration > File Management > File Operations**. | |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | Under Operation Type, select **Update File**. | |
| **Step 4** | Next, select the Destination File Type from the following options: | • Running Configuration<br>• Startup Configuration |
| **Step 5** | For the Copy Method, select from one of the following options: | • HTTP/HTTPS<br>• USB<br>• Internal Flash |
| **Step 6** | Next, in the File Name section, click the Browse button to locate and select the configuration file. | The switch will apply the configuration changes immediately if the configuration was applied directly to the running configuration.<br>If the configuration was applied to the startup configuration, you will need to reboot the switch for the configuration changes to take place.<br>It's important to note that restoring a configuration file will overwrite the current configuration on the switch. Before restoring a configuration file, make sure to back up the current configuration to avoid losing any changes that were made since the backup. |

# File Directory

The File Directory page displays the system files existing in the system.

### Procedure

**Step 1** Click **Administration** > **File Management** > **File Directory**.

**Step 2** If required, enable Auto Mirror Configuration. This enables the automatic creation of mirror configuration files. When disabling this feature, the mirror configuration file, if it exists, is deleted.

**Step 3** Select the drive from which you want to display the files and directories. The following options are available:

- Flash—Display all files in the root directory of the management station.
- USB—Display files on the USB drive.

**Step 4** Click **Go** to display the following fields:

- File Name—Type of system file or actual name of file depending on the file type.
- Permissions—Read/write permissions of the user for the file.
- Size—Size of file.
- Last Modified—Date and time that file was modified.

- Full Path—Path of file.

**Step 5** Click the **Refresh** icon to refresh the data. If you would like to delete a file, select the file and click the **Delete** icon.

**Step 6** Click **Apply** to save the settings.

# DHCP Auto Update

The Auto Configuration/Image Update feature provides a convenient method to automatically configure switches in a network and upgrade their firmware. This process enables the administrator to remotely ensure that the configuration and firmware of these devices in the network are up to date.

### Procedure

**Step 1** Click **Administration** > **File Management** > **DHCP Auto Update**.

**Step 2** Configure the following:

| | |
|---|---|
| Auto Configuration Via DHCP | Check **Enable** to enable the auto configuration via DHCP. The Auto Configuration feature provides a convenient method to automatically configure switches in a network and upgrade their firmware. |
| Download Protocol | Select the download protocol from the following options:<br>• Auto By File Extension—(Default) Files with this extension are downloaded using SCP (over SSH), while files with other extensions are downloaded using TFTP.<br>• TFTP Only—The download is done through TFTP, regardless of the file extension of the configuration file name.<br>• SCP Only—The download is done through SCP (over SSH), regardless of the file extension of the configuration file name. |
| Image Auto Update via DHCP: | Check **Enable** to enable image auto update via DHCP. The Image Auto Update feature provides a convenient method to automatically update switches in a network and upgrade their firmware. |
| Download Protocol | Select the download protocol from the following options:<br>• Auto By File Extension—(Default) Files with this extension are downloaded using SCP (over SSH), while files with other extensions are downloaded using TFTP.<br>• TFTP Only—The download is done through TFTP, regardless of the file extension of the configuration file name.<br>• SCP Only—The download is done through SCP (over SSH), regardless of the file extension of the configuration file name. |

**Step 3** Select the SSH settings for SCP.

| | |
|---|---|
| Remote SSH Server Authentication: | Click the link to navigate to the SSH Server Authentication page. There you can enable authentication of the SSH server to be used for the download and enter the trusted SSH server if required. |
| SSH Client Authentication | • Click on the **System Credentials** to enter user credentials in the SSH User Authentication page. |
| Backup Server Definition | Select from the following options:<br>• By IP Address<br>• By Name |
| IP Version | Select from the following options:<br>• Version 6<br>• Version 4 |
| IPv6 Address Type | Select from the following options:<br>• Link Local—A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network.<br>• Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks. |
| Link Local Interface | If for the IPv6 address type, you selected Link Local, select the interface from the drop down list. |
| Backup Server IP Address/Name | Enter the name of the backup configuration file. |
| Backup Configuration File Name | Enter the name of the backup configuration file (0- 160 characters used) |
| Backup Indirect Image File Name | Enter the name of backup indirect image file (0- 160 characters used). |
| Last Auto Configuration Server IP Address | The address of the last auto configuration server IP address is displayed. |
| Last Auto Configuration File Name | The name of the last auto configuration file is displayed. |

**Note**
DHCP Auto Configuration / Image is operational only when the IP Address configuration is dynamic.

**Step 4** Click **Apply** to save your settings.

# Cisco Business Dashboard Settings

Cisco Business Dashboard helps you monitor and manage your Cisco 100 to 500 Series network with the use of the Cisco Business Dashboard Manager. The Cisco Business Dashboard Manager is an add-on that

automatically discovers your network and allows you to configure and monitor all supported Cisco 100 to 500 Series devices such as Cisco switches, routers, and wireless access points.

You can view the Cisco Business Dashboard by clicking Request a Demo

Cisco Business Dashboard Manager is a distributed application which is comprised of two separate components or applications: one or more Probes referred to as Cisco Business Dashboard Probe and a single Manager called Cisco Business Dashboard Manager. An instance of Cisco Business Dashboard Probe is installed at each site in the network, performs network discovery and communicates directly with each Cisco device.

**Note** For detailed instructions on how to setup the Cisco Business Dashboard Manager and Probe, please consult the Cisco Business Dashboard Quick Start Guide.

https://cisco.com/go/cbd-docs

Complete the following steps on the switch graphical user interface (GUI) to enable a Probe connection to a Dashboard, configure the Organization and Network name, and other information required to allow connection to the Dashboard:

### Procedure

**Step 1** Click **Administration** > **Cisco Business Dashboard Settings**.

**Step 2** Configure the following:

| | |
|---|---|
| Probe Operation | Check to enable the Cisco Business Dashboard Probe operation. |
| Probe Status | Displays the status of the CBD probe. Possible value are Active, Inactive or Fault.<br>If the probe status is Active then alongside the probe status "Active" the probe mode will also be displayed as follows:<br>• Active (Probe Managed) - The Probe performs network discovery and communicates directly with each managed device on behalf of the Dashboard.<br>In one network you should only enable one Probe.<br>• Active (Direct Managed) - Direct managed devices will discover other devices in the broader network and connect those devices to the Dashboard automatically then those devices become manageable. You may optionally have the dashboard explicitly search the IP address ranges to discover network devices, which can be in other VLANs or subnets.<br>Direct managed network is recommended if all your devices support direct management. |
| Probe Version | Displays the version of the Cisco Business Dashboard probe. |
| Logging Threshold | Select one of the following options (Information, Debug, Warning, or Error) from the drop-down list to limit the level of messages logged by the Cisco Business Dashboard probe agent. Only messages with the specified level or higher will be logged. |

| | |
|---|---|
| All Module Logging | Check to enable. This logs all communication and events between all modules. |
| Call Home Logging | Check to enable. This logs all communication between the Probe and Manger. |
| Discovery Logging | Check to enable. This logs the device discovery events and topology discovery. |
| Services Logging | Check to enable. This logs the message translation between northbound and southbound. |
| System Logging | Check to enable. This logs the core system process not covered by any of the other logs. |
| Northbound Logging | Check to enable. This logs the communication between the Manager and the Probe. |
| Southbound Logging | Check to enable. This logs the low level communication between the Probe and devices. |
| Dashboard Connection | Check to enable connection. |
| Dashboard Status | Displays the status (Connected or Disconnected) of the Cisco Business Dashboard Manager.<br>If the Dashboard Status is "Disconnected" an error reason will be displayed. Here are some examples:<br>• Certificate-error- unspecified certificate verification error<br>• Certificate-error- certificate is not yet valid<br>• Certificate-error- certificate has expired<br>• Certificate-error- certificate verify failed<br>• Connection-error- Host not found (authoritative)<br>• Connection-error- No route to host |
| Dashboard Definition | Define the address of the Cisco Business Dashboard. Select one of the following:<br>• By IP address- this option requires you to enter a valid IP address to the IP Address/Name field.<br>• By Name- this option requires you to enter a host name to the IP Address/Name field. |
| IP Address/Name | Enter the name or IP address of the Cisco Business Dashboard. |
| Dashboard Port | Specify one of the following TCP ports to connect to the Dashboard.<br>• Use Default (443).<br>• User Defined (Range: 1-65535). This option is available only if a valid address is entered in the Dashboard Address field. |
| Connection Setup | Specify one of the following connection setups:<br>• Online with Web Browser<br>• Offline with Access Key |

| | |
|---|---|
| Access Key ID | The Access Key ID field consists of 24 hexadecimal digits. Note that the field should only allow the input of hexadecimal characters. |
| Access Key Secret | Specify the secret to use for authentication. It can be Encrypted or in Plaintext format. The Plaintext format is specified as an alphanumeric string without white-spaces (up to 160 chars). The Key ID and Secret settings must be set together.<br>**Note**<br>When applying, if the Key ID field is empty and the Secret field is not, or if the Secret field is empty and the Key ID field is not, the following error message is displayed: "Key ID and Secret must be set together". |

**Step 3** Click **Apply** to save the setting to the running configuration.

**Note**
The fields Organization Name, Network Name, Dashboard Address, Key ID cannot be modified if Dashboard Connection setting is enabled. To modify any of these settings clear the Dashboard Connection check box, click **Apply**, and redo steps 2-4 above.

**Display Sensitive Data as Plaintext**- Click to display the sensitive data a plain text.

**Reset Connection** - click to disconnect the current connection with the Dashboard, flush the Cisco Business Dashboard Probe cached data, and then attempt to reconnect to the Dashboard. A confirmation message is displayed before the operation starts. This control is enabled only if the Dashboard Connection and Probe Operation are enabled.

**Note**
The Reset Connection is only enabled if the Dashboard Connection and Probe Operation check boxes are checked.

**Clear Probe Database**- Click to clear the probe data. It is enabled only if the Probe Operation checkbox is unchecked (and has been unchecked since the screen loaded). Otherwise, the button is disabled with the following tooltip: "Probe Operation must be disabled prior to clearing probe database".

**Note**
Many factors affect the number of network devices and clients that the Cisco Business Dashboard Probe on a switch can manage. We recommend that a probe on a switch manage no more than 15 network devices (switches, routers, and wireless access points) and no more than 150 connected clients. If your network is more complex, we recommend that you use other platforms for the Cisco Business Dashboard Probe. For more information about Cisco Business Dashboard, go to https://www.cisco.com/c/en/us/products/cloud-systems-management/business-dashboard/index.html.

# Plug-n-Play (PNP)

Installation of new networking devices or replacement of devices can be expensive, time-consuming and error-prone when performed manually. Typically, new devices are first sent to a central staging facility where the devices are unboxed, connected to a staging network, updated with the right licenses, configurations and images; then packaged and shipped to the actual installation location. After these processes are completed, experts must travel to the installation locations to perform the installation. Even in scenarios where the devices are installed in the NOC/Data Center itself, there may not be enough experts for the sheer number of devices. All these issues contribute to delays in deployment and add to the operational costs.

### Connecting to PNP Server

To allow the switch to connect to the PnP server, a discovery process takes place, in which the switch discovers the PNP server address/url. There are multiple discovery methods, and they are executed by the switch according to the sequence detailed below. If a PnP server is discovered by a certain method, the discovery process is completed and the rest of the methods are not executed:

1. User configured address- the PnP server URL or IP address are specified by the user.
2. Address received from DHCP response option 43- the PnP server URL or IP address are received as part of option 43 in the DHCP response
3. DNS resolution of host name "pnpserver"- the PnP server IP addressed is obtained via DNS server resolution of host name “pnpserver”.
4. Cisco Plug and Play Connect - a redirection service that allows full “out of the box” PNP server discovery which runs over HTTPs.

The switch contacts the redirection service using the FQDN “devicehelper.cisco.com”.

### Cisco PnP Connect Prerequisites

To allow Cisco Plug and Play Connect operation, the user needs to create devices and controller profiles in Plug and Play Connect (navigate to https://software.cisco.com and click the PnP Connect link). Note that a Cisco Smart Account is required to use PnP Connect. To create or update a Smart Account, see the Administration section of https://software.cisco.com.

In addition, the following prerequisites are required to be met on the switch itself:

- The PNP server was not discovered by the other discovery methods
- The device is able to successfully resolve the name devicehelper.cisco.com (either static configuration or using DNS server)
- System time was set using one of the following methods
  - Time was updated by an SNTP server
  - Clock was set manually by user
  - Time was preserved across resets by Real Time Clock (RTC).

### CA-Signed Certificate based Authentication

Cisco distributes certificates signed by a signing authorities in .tar file format and signs the bundle with Cisco Certificate Authority (CA) signature. This certificate bundle is provided by Cisco infoSec for public downloads on cisco.com.



**Note** If the PNP server discovery is based on Cisco PnP Connect, the trust-pool is downloaded from following: http://www.cisco.com/security/pki/trs/ios_core.p7b.

If the PNP server discovery is based on DHCP option 43, use the “T<Trust pool CA bundle URL>;” parameter in DHCP option 43 to provide the URL for downloading the trust pool. The certificates from this bundle can

be installed on the Cisco device for server-side validation during SSL handshake. It is assumed that the server uses a certificate, which is signed by one of the CA that is available in the bundle.

The PnP agent uses the built-in PKI capability to validate the certificate bundle. As the bundle is signed by Cisco CA, the agent is capable of identifying a bundle that is tampered before installing the certificates on the device. After the integrity of the bundle is ensured by the agent, the agent installs the certificates on the device. After the certificates are installed on the device, the PnP agent initiates an HTTPs connection to the server without any additional steps from the server.



**Note** The device also supports a built in certificate bundle which is installed as part of the bootup process. this bundle can be used to validate PNP server. If a Bundle is downloaded based on Cisco PnP Connect information then the certificates from the downloaded bundle are installed and the certificates based on the built in bundle are un-installed.



**Note** In addition to validating PNP certificate based on installed CA certificate the PNP Agent also validates that the certificate's Common Name/Subject Alternate Name (CN/SAN) matches the host name/IP address of the PNP server. If they don't match validation of certificate is rejected.

### Cisco PnP DHCP Option 43 Usage Guidelines

DHCP option 43 is a vendor specific identifier which is one of the methods that can be used by the PnP agent to locate and connect to the PnP server (see Cisco Plug-n-Play for more information).

The following provides Information on configuration of Option 43 to allow proper configuration on DHCP server.

Option 43 includes the following fields/parameters:

*<DHCP-typecode><feature-opcode><version><debug-option>;<arglist>*

The <arglist> parameter should use the following syntax:

*B<IP address type>;I<IP address>;J<Port>;K<Transport protocol>;T<Trust pool CA bundle URL>;Z<SNTP server IP address>*

The following table details the description and usage of option 43 fields

| Parameter | Description |
|---|---|
| DHCP-typecode | DHCP sub-option type. The DHCP sub-option type for PnP is 5. |
| Feature-opcode | Feature operation code – can be either Active (A) or Passive (P). The feature operation code for PnP is Active (A) which implies that PnP agent initiates a connection to the PnP server. If the PnP server cannot be reached, PnP agent retries until it makes a connection. |
| Version | Version of template to be used by PnP agent. Must be 1. |

| Parameter | Description |
|---|---|
| Debug-option | Turns ON or OFF the debug messages during the processing of the DHCP Option 43:<br>D – debug option is ON; N – debug option is OFF. |
| K | Transport protocol to be used between PnP agent and PnP server:<br>4 - HTTP or 5 – HTTPS. |
| B | IP address type of PnP server IP address specified with the letter code<br>'I':<br>1- host, 2- IPv4, 3- IPv6 |
| I | IP address or host name of PnP server. If host name is specified, DNS related options must be present in the DHCP server to allow for successful use of host name. |
| T | URL of trust pool CA bundle. You can get the CA bundle from a Cisco Business Dashboard, or from a TFTP server.<br>• When using Cisco Business Dashboard, use the following URL format:<br>http://*CBD IP address or domain name/ca/trustpool/CA_bundle_name*<br>• When using TFTP Server, use the following URL format: tftp://*tftp server IP/CA_bundle_name* |
| Z | SNTP server IP address. You must sync the clock before configuring a trust pool.<br>**Note**<br>The switch clock is considered synchronized if it was updated by any SNTP server supported by the switch (by default, user configured or in Z parameter) or set manually by the user. This parameter is required when using trust pool security if the switch can not reach any other SNTP server. For example, for an out-of-the box switch with factory default configuration but no Internet connectivity to reach the default SNTP servers. |
| J | Port number HTTP=80 HTTPS=443 |

**Examples for Option 43 usage:**

- The following format is used for PnP connection setup using HTTP:

```
option 43 ascii 5A1N;K4;B2;I10.10.10.3;J80
```

- The following format is used for PnP connection setup on top of HTTPS, directly using a trust pool. HTTPS can be used when the trust pool CA bundle is downloaded from a Cisco Business Dashboard and the Cisco Business Dashboard server certificate was issued by a 3rd party (not self signed). In the

example below “10.10.10.3” is the Cisco Business Dashboard IP address. Optionally, you can specify a domain name:

```
option 43 ascii
5A1N;K5;B2;I10.10.10.3;Thttp://10.10.10.3/ca/trustpool/ios.p7b;Z10.75.166.1
```

# PNP Settings

To configure PNP settings, follow these steps:

### Procedure

**Step 1** Click **Administration** > **PNP** > **PNP Settings**.

**Step 2** Configure PNP by entering information in the following fields:

| | |
|---|---|
| PNP State | Check to enable. |
| PNP Transport / Settings Definition | Select one of the following options for locating configuration information, regarding the transport protocol to use, the PNP server address and the TCP port to use:<br>• Default Settings—If this option is selected, the PNP settings are then taken from DHCP option 43. If settings aren’t received from DHCP option 43, the following default values are used: default transport protocol HTTP, DNS name "pnpserver" for PNP server and the port related to HTTP. If the “pnpserver” name is not resolved by DNS, then Cisco Plug and Play Connect service is used, using DNS name “devicehelper.cisco.com”. When selecting the Default Settings option, all fields in PNP Transport section are grayed out. If both PNP agent and DHCP Auto Configuration/Image Update are enabled on device- in case he DHCP reply includes, in addition to option 43, options related to config or image file name, then device ignores received option 43.<br>• Manual Settings—Manually set the TCP port and server settings to use for PNP transport. |
| Transport Protocol | Select the transport protocol, HTTP or HTTPS. |
| TCP Port | Number of the TCP port. This is entered automatically by the system: 80 for HTTP. |
| Server Definition | Select whether to specify the PNP server By IP address or By name. |
| IP Version | Select the supported IP format.<br>• Version 6—IPv6<br>• Version 4—IPv4 |

| | |
|---|---|
| Server IPv6 Address Type | Select one of the following options, if the IP version type is IPv6:<br>• 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.<br>• Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks. |
| Link Local Interface | If the source IPv6 address type is Link Local, select from where it is received. |
| Server IP Address/Name | Enter the IP address or domain name of the PNP server. |
| PNP User / User Definition | User information to be sent in PNP packets sent to the server. Select one of the following options:<br>• Default Settings—When selecting this option, the PNP username and password settings are taken from DHCP option 43. If this option is selected the username and password fields are grayed out.<br>• Manual Settings—Select to manually configure PNP username and password. |
| User Name | Username to be entered in the PNP packets. |
| Password | Password in either Encrypted or Plaintext form. |
| PNP Behavior Settings/Reconnection Interval | If you select User Defined, set the interval (in seconds) before attempting to reconnect the session after the connection is lost. |
| Discovery Timeout | Specifies the time to wait, in seconds, before attempting discovery again after a discovery of the PNP server failed. |
| Timeout Exponential Factor | Value that triggers the discovery attempt exponentially. By multiplying the previous timeout value by an exponential value and applying the result as timeout (if value is smaller than max timeout value). |
| Max Discovery Timeout | Maximum value of timeout. Must be greater than the Discovery Timeout value. |
| Watchdog Timeout | Interval of time to wait for a reply from a PnP or file server during an active PNP session (for example during a file download process). |

**Step 3** Click **Apply**. The parameters are copied to the Running Configuration file.

Click **Display Sensitive Data as Plaintext** to display the password if it's encrypted.

# PNP Session

The PNP Session screen displays the value of the PNP parameters currently in effect. The source of the parameter is displayed in parenthesis where relevant.

To display information about PNP parameters, follow these steps:

### Procedure

Click **Administration > PNP > PNP Session**.

The following fields are displayed:

- Administrative Status—Whether PNP is enabled or not.
- Operational Status—Is PNP operational.
- PNP Agent State—Indicates whether there's an active PNP session. The possible values are Discovery Wait; Discovery; Not Ready; Disabled; Session; Session Wait.
- Transport Protocol– Displays the PNP agent session information.
- TCP Port—TCP port of the PNP session
- Server IP Address—IP address of PNP server
- Username—Username to be sent in PNP packets.
- Password MD5—Password to be sent in PNP packets.
- Session Interval Timeout—Session Interval timeout configured (appears only when PNP Agent State is waiting).
- Remaining Timeout—Value of remaining timeout.



**Note** Click the **Resume** button to immediately take the PnP agent out of the waiting state, in the following way:

- If the agent is in the Discovery Waiting state, it's set to the Discovery state.
- If the agent is in the PnP Session Waiting state, it's set to the PnP Session state.

# Reboot

Some configuration changes, such as enabling jumbo frame support, require the system to be rebooted before they take effect. However, rebooting the device deletes the Running Configuration, so it's critical to save the Running Configuration as the Startup Configuration before rebooting. Clicking Apply doesn't save the configuration to the Startup Configuration. section.

To reboot the device, follow these steps:

### Procedure

**Step 1** Click **Administration** > **Reboot**.

**Step 2** Click **Reboot** to reboot the device. A pop-up will appear to confirm reboot. Click **OK**

Since any unsaved information in the Running Configuration is discarded at reboot, you must click **Save** to preserve the current configuration across the boot process. If the Save option isn't displayed, the Running Configuration matches the Startup Configuration and no action is necessary.

**Step 3** Select from one of the following reboot options:

- • Immediate—Reboot immediately.
  - Date—Enter the date (month/day) and time (hour and minutes) of the schedule reboot. This schedules a reload of the software to take place at the specified time (using a 24-hour clock).

    **Note**
    This option can only be used if the system time has either been set manually or by SNTP.

  - In—Enter the specified number of days, hours and minutes to reboot the device. The maximum amount of time that can pass is 24 days.

**Step 4** Check Restore to Factory Defaults restore factory default setting during the reboot process.

**Step 5** Check Clear Startup Configuration File to clear the configuration file.

**Step 6** Click **Cancel Reboot** to cancel a scheduled reboot.

# Discovery - Bonjour

As a Bonjour client, the device broadcasts Discovery Bonjour protocol packets to directly connected IP subnets. The device can be discovered by a network management system or other third-party applications. By default, Bonjour is enabled on the Management VLAN.

To configure Bonjour, follow these steps:

### Procedure

**Step 1** Click **Administration** > **Discovery - Bonjour**.

**Step 2** Check **Enable** to enable Discovery Bonjour globally.

**Step 3** To enable Bonjour on a specific interface, click **Add.**

**Step 4** Select the interface (Port, LAG, or VLAN) and configure the interface.

**Step 5** Click **Apply** to update the Running Configuration file.

**Note**
When Bonjour is enabled, it sends Discovery Bonjour packets to interfaces with IP addresses associated with Bonjour on the Bonjour Discovery Interface Control table.

**Step 6** Click **Delete** to disable Bonjour on an interface.

# Discovery - LLDP

LLDP is a protocol that enables network managers to troubleshoot and enhance network management in multi-vendor environments. LLDP standardizes methods for network devices to advertise themselves to other systems, and to store discovered information. LLDP enables a device to advertise its identification, configuration, and capabilities to neighboring devices that then store the data in a Management Information Base (MIB).

LLDP is a link layer protocol. By default, the device terminates and processes all incoming LLDP packets as required by the protocol. This section describes how to configure LLDP and covers the following topics:

## Properties

The Properties page enables entering LLDP general parameters, such as enabling/disabling the feature globally and setting timers. To enter LLDP properties, proceed as follows:

### Procedure

**Step 1** Click **Administration** > **Discovery - LLDP** > **Properties**.

**Step 2** Enter the parameters.

| | |
|---|---|
| LLDP Status | Select to enable LLDP on the device (enabled by default). |
| LLDP Frames Handling | If LLDP isn't enabled, select one of the following options:<br>• Filtering—Delete the packet.<br>• Flooding—Forward the packet to all VLAN members |
| TLV Advertise Interval | Select one of the following options:<br>• Use Default—Use default values.<br>• User Defined—Enter a value. |
| Topology Change SNMP Notification Interval | Select one of the following options:<br>• Use Default—Use default values.<br>• User Defined—Enter a value. |
| Hold Multiplier | Select one of the following options:<br>• Use Default—Use default values.<br>• User Defined—Enter a value. |

| | |
|---|---|
| Reinitializing Delay | Select one of the following options:<br>• Use Default—Use default time.<br>• User Defined—Enter a time |
| Transmit Delay | Select one of the following options:<br>• Use Default—Use default time.<br>• User Defined—Enter a time |
| Chassis ID Advertisement | Select one of the following options for advertisement in the LLDP messages:<br>• MAC Address—Advertise the MAC address of the device.<br>• Host Name—Advertise the host name of the device. |

**Step 3** In the LED-MED Properties for the Fast Start Repeat Count field, enter the number of times LLDP packets are sent when the LLDP-MED Fast Start mechanism is initialized. This occurs when a new endpoint device links to the device. For a description of LLDP MED, refer to the LLDP MED Network Policy section.

**Step 4** Click **Apply**. The LLDP properties are added to the Running Configuration file.

# Port Settings

**Note** This setting is only available in the Advanced Mode view.)

The LLDP Port Settings page enables LLDP and SNMP notification per port. The LLDP-MED TLVs can be configured in the LLDP MED Port Settings, on page 42.

To define the LLDP port settings, follow these steps:

### Procedure

**Step 1** Click **Administration** > **Discovery - LLDP** > **Port Settings**.

This page contains the port LLDP information.

**Step 2** Select a port and click **Edit.**

**Step 3** Configure the following fields:

| | |
|---|---|
| Interface | Select the port to edit. |

| | |
|---|---|
| Administrative Status | Select the LLDP publishing option for the port.<br>• Tx Only—Publishes but doesn't discover.<br>• Rx Only—Discovers but doesn't publish.<br>• Tx & Rx—Publishes and discovers.<br>• Disable—Indicates that LLDP is disabled on the port. |
| SNMP Notification | Select **Enable** to send notifications to SNMP notification recipients. |
| Available/Selected Optional TLVs | Select the options to be published by the device:<br>• Port Description—Information about the port.<br>• System Name—System's assigned name.<br>• System Description—Description of the network entity.<br>• System Capabilities—Primary functions of the device, and whether these functions are enabled on the device.<br>• 802.3 MAC-PHY—Duplex and bit rate capability and the current duplex and bit rate settings of the sending device.<br>• 802.3 power via MDI—Maximum power transmitted via MDI<br>• 802.3 Link Aggregation—Whether the link (associated with the port on which the LLDP PDU is transmitted) can be aggregated.<br>• 802.3 Maximum Frame Size—Maximum frame size capability of the MAC/PHY implementation<br>• 4-Wire Power via MDI—(relevant to PoE ports supporting 60W PoE) Proprietary Cisco TLV defined to support power over Ethernet that allows for 60 watts power (standard support is up to 30 watts).<br>Management Address Optional TLV |
| Advertisement Mode | Select one of the following ways to advertise the IP management address of the device:<br>• Auto Advertise—Specifies that the software automatically chooses a management address to advertise from all the IP addresses of the device. In case of multiple IP addresses, the software chooses the lowest IP address among the dynamic IP addresses. If there are no dynamic addresses, the software chooses the lowest IP address among the static IP addresses.<br>• None—Select this option if no advertisement mode is desired.<br>• Manual Advertise—Select this option and the management IP address to be advertised. |
| IP Address | If Manual Advertise was selected, select the Management IP address from the addresses provided. |

| | |
|---|---|
| PVID | Select to advertise the PVID in the TLV. |
| VLAN ID | Select which VLANs will be advertised. |
| Protocol IDs | Select which protocols will be advertised. |
| Selected Protocol IDs | Select the protocols to be used in the Protocols IDs box and move them to the Selected Protocols ID box. |

**Step 4** Enter the relevant information, and click **Apply**. The port settings are written to the Running Configuration file.

# LLDP MED Network Policy

The LLDP-MED network policy is a related set of configuration settings for a specific real-time application such as voice, or video. A network policy, if configured, can be included in the outgoing LLDP packets to the attached LLDP media endpoint device. The media endpoint device must send its traffic as specified in the network policy it receives. For example, a policy can be created for VoIP traffic that instructs VoIP phone to:

- Send voice traffic on VLAN 10 as tagged packet and with 802.1p priority 5.
- Send voice traffic with DSCP 46.

Network policies are associated with ports by using the LLDP MED Port Settings, on page 42. An administrator can manually configure one or more network policies and the interfaces where the policies are to be sent. It is the administrator's responsibility to manually create the VLANs and their port memberships according to the network policies and their associated interfaces.

In addition, an administrator can instruct the device to automatically generate and advertise a network policy for voice application based on the voice VLAN maintained by the device. Refer the Auto Voice VLAN section for details on how the device maintains its voice VLAN.

To define an LLDP MED network policy, follow these steps:

### Procedure

**Step 1** Click **Administration** > **Discovery - LLDP** > **LLDP MED Network Policy.**

This page contains previously-created network policies.

**Step 2** Select **Auto** for LLDP-MED Network Policy for Voice Application if the device is to automatically generate and advertise a network policy for voice application based on the voice VLAN maintained by the device.

**Note**
When this box is checked, you may not manually configure a voice network policy.

**Step 3** Click **Apply** to add this setting to the Running Configuration file.

**Step 4** To define a new policy, click **Add**.

**Step 5** Enter the values:

- Network Policy Number—Select the number of the policy to be created.

- Application—Select the type of application (type of traffic) for which the network policy is being defined.
- VLAN ID—Enter the VLAN ID to which the traffic must be sent. (Range 0 - 4095)
- VLAN Type—Select whether the traffic is Tagged or Untagged.
- User Priority—Select the traffic priority applied to traffic defined by this network policy. This is the CoS value.
- DSCP Value—Select the DSCP value to associate with application data sent by neighbors. This value informs them how they must mark the application traffic they send to the device.

**Step 6** Click **Apply**. The network policy is defined.

**Note**
You must manually configure the interfaces to include the desired manually-defined network policies for the outgoing LLDP packets using the LLDP MED Port Settings.

# LLDP MED Port Settings



**Note** This setting is only available in the Advanced Mode view.

The LLDP MED Port Settings page enables configuration of the LLDP-MED TLVs. Network policies are configured using the LLDP MED Network Policy page.



**Note** If LLDP-MED Network Policy for Voice Application is Auto and Auto Voice VLAN is in operation, then the device automatically generates an LLDP-MED Network Policy for Voice Application for all the LLDP ports. LLDP-MED enabled and are members of the voice VLAN.

To configure LLDP MED on each port, proceed as follows:

**Procedure**

**Step 1** Click **Administration** > **Discovery - LLDP** > **LLDP MED Port Settings**.

**Step 2** The message at the top of the page indicates whether the generation of the LLDP MED Network Policy for the voice application is automatic or not. Click on the link to change the mode.

**Step 3** To associate additional LLDP MED TLV and/or one or more user-defined LLDP MED Network Policies to a port, select it, and click **Edit.**

**Step 4** Enter the parameters:

- Interface—Select the interface to configure.
- LLDP MED Status—Enable/disable LLDP MED on this port.

- SNMP Notification—Select whether SNMP notification is sent on a per-port basis when an end station that supports MED is discovered.
- Selected Optional TLVs—Select the TLVs that can be published by the device by moving them from the Available Optional TLVs list to the Selected Optional TLVs list.
- Selected Network Policies—Select the LLDP MED policies to be published by LLDP by moving them from the Available Network Policies list to the Selected Network Policies list. To include one or more user-defined network policies in the advertisement, you must also select **Network Policy** from the Available Optional TLVs.

**Note**
The following fields must be entered in hexadecimal characters in the exact data format that is defined in the LLDP-MED standard (ANSI-TIA-1057_final_for_publication.pdf):

- Location Coordinate—Enter the coordinate location to be published by LLDP.
- Location Civic Address—Enter the civic address to be published by LLDP.
- Location ECS ELIN—Enter the Emergency Call Service (ECS) ELIN location to be published by LLDP.

**Step 5** Click **Apply**. The LLDP MED port settings are written to the Running Configuration file.

**Step 6** Click on LLDP Local Information Detail to display the LLDP Local Information.

# LLDP Port Status

The LLDP Port Status page contains the LLDP global information for every port.

**Procedure**

**Step 1** To view the LLDP port status, click **Administration** > **Discovery - LLDP** > **LLDP Port Status**.

Information for all ports is displayed.

**Step 2** Select a specific port and click **LLDP Local Information Detail** to see the details of the LLDP and LLDP-MED TLVs sent out to the port.

**Step 3** Select a specific port and click **LLDP Neighbor Information Detail** to see the details of the LLDP and LLDP-MED TLVs received from the port.

**LLDP Port Status Global Information**

- Chassis ID Subtype—Type of chassis ID (for example, MAC address).
- Chassis ID—Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the device appears.
- System Name—Name of device.
- System Description—Description of the device (in alpha-numeric format).
- Supported System Capabilities—Primary functions of the device, such as Bridge, WLAN AP, or Router.
- Enabled System Capabilities—Primary enabled function(s) of the device.

- Port ID Subtype—Type of the port identifier that is shown.

**LLDP Port Status Table**

- Interface—Port identifier.
- LLDP Status—LLDP publishing option.
- LLDP MED Status—Enabled or disabled.
- Local PoE ((Power Type, Power Source, Power Priority, Power Value)—Local PoE information advertised.
- Remote PoE (Power Type, Power Source, Power Priority, Power Value)—PoE information advertised by the neighbor.
- # of neighbors—Number of neighbors discovered.
- Neighbor capability of 1st device—Displays the primary functions of the neighbor; for example: Bridge or Router.

# LLDP Local Information

To view the LLDP local port status advertised on a port, follow these steps:

**Procedure**

**Step 1** Click **Administration** > **Discovery - LLDP** > **LLDP Local Information**.

**Step 2** Select the interface for which the LLDP local information is to be displayed.

The LLDP Local Information page contains the following fields:

**Global**

- Chassis ID Subtype—Type of chassis ID. (For example, the MAC address.)
- Chassis ID—Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the device appears.
- System Name—Name of device.
- System Description—Description of the device (in alpha-numeric format).
- Supported System Capabilities—Primary functions of the device, such as Bridge, WLAN AP, or Router.
- Enabled System Capabilities—Primary enabled function(s) of the device.
- Port ID Subtype—Type of the port identifier that is shown.
- Port ID—Identifier of port.
- Port Description—Information about the port, including manufacturer, product name and hardware/software version.

**Management Address**

- IPv4 Address—IPv4 returned address most appropriate for management use.

- IPv6 Global Address—IPv6 returned global address most appropriate for management use.
- IPv6 Link Local Address—IPv6 returned link local address most appropriate for management use.

**MAC/PHY Details**

- Auto-Negotiation Supported—Port speed auto-negotiation support status. The possible values are True and False.
- Auto-Negotiation Enabled—Port speed auto-negotiation active status. The possible values are True and False.
- Auto-Negotiation Advertised Capabilities—Port speed auto-negotiation capabilities, for example, 1000BASE-T half duplex mode, 100BASE-TX full duplex mode.
- Operational MAU Type—Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network; for example, 100BASE-TX full duplex mode.

**802.3 Details**

- 802.3 Maximum Frame Size - The maximum supported IEEE 802.3 frame size.

**802.3 Link Aggregation**

- Aggregation Capability—Indicates whether the interface can be aggregated.
- Aggregation Status—Indicates whether the interface is aggregated.
- Aggregation Port ID—Advertised aggregated interface ID.

**802.3 Energy Efficient Ethernet (EEE)**

- Local Tx—Indicates the local link partner's reflection of the remote link partner's Tx value.
- Local Rx—Indicates the local link partner's reflection of the remote link partner's Rx value.
- Remote Tx Echo—Indicates the time (in micro seconds) that the transmitting link partner waits before it starts transmitting data after leaving Low Power Idle (LPI mode).
- Remote Rx Echo—Indicates the time (in micro seconds) that the receiving link partner requests that the transmitting link partner waits before transmission of data following Low Power Idle (LPI mode).

**802.3 Power via MDI**

- MDI Power Support Port Class—Advertised power support port class.
- PSE MDI Power Support—Indicates if MDI power is supported on the port.
- PSE MDI Power State—Indicates if MDI power is enabled on the port.
- PSE Power Pair Control Ability—Indicates if power pair control is supported on the port.
- PSE Power Pair—Power pair control type supported on the port.
- PSE Power Class—Advertised power class of the port.
- Power Type—Type of pod device connected to the port.
- Power Source—Port power source.
- Power Priority—Port power priority

- PD Requested Power Value—Amount of power allocated by the PSE to the PD.
- PSE Allocated Power Value—Amount of power allocated to the sourcing equipment (PSE).

**4-Wire Power via MDI**

- 4-Pair PoE Supported—Indicates system and port support enabling the 4-pair wire (true only for specific ports that have this HW ability).
- Spare Pair Detection/Classification Required—Indicates that the 4-pair wire is needed.
- PD Spare Pair Desired State—Indicates a pod device requesting to enable the 4-pair ability.
- PD Spare Pair Operational State—Indicates if the 4-pair ability is enabled or disabled.

**MED Details**

- Capabilities Supported—MED capabilities enabled on the port.
- Current Capabilities—MED TLVs advertised by the port.
- Device Class—LLDP-MED endpoint device class. The possible device classes are:
  - Endpoint Class 1—Indicates a generic endpoint class, offering basic LLDP services.
  - Endpoint Class 2—Indicates a media endpoint class, offering media streaming capabilities as well as all Class 1 features.
  - Endpoint Class 3—Indicates a communications device class, offering all Class 1 and Class 2 features plus location, 911, Layer 2 switch support and device information management capabilities.

**Extended PSE Information**

- PoE Device Type—Port PoE type, for example, PD/PSE.
- PoE Power Source—Port’s power source.
- PoE Power Priority—Port’s power priority.
- PoE Power Value—Port’s power value.

**Inventory Information**

- Hardware Revision –Hardware version.
- Firmware Revision—Firmware version.
- Software Revision—Software version.
- Serial Number—Device serial number.
- Manufacturer Name—Device manufacturer name.
- Model Name—Device model name.
- Asset ID—Asset ID.

**Location Information**

Enter the following data structures in hexadecimal as described in section 10.2.4 of the ANSI-TIA-1057 standard:

- Civic—Civic or street address.
- Coordinates—Location map coordinates—latitude, longitude, and altitude.
- ECS ELIN—Device's Emergency Call Service (ECS) Emergency Location Identification Number (ELIN).

**Network Policy Table**

- Application Type—Network policy application type, for example, Voice.
- VLAN ID—VLAN ID for which the network policy is defined.
- VLAN Type—VLAN type, Tagged or Untagged, for which the network policy is defined.
- User Priority—Network policy user priority.
- DSCP—Network policy DSCP.

# LLDP Neighbor Information

The LLDP Neighbor Information page contains information that was received from neighboring devices. After timeout (based on the value received from the neighbor Time To Live TLV during which no LLDP PDU was received from a neighbor), the information is deleted.

To view the LLDP neighbors information, follow these steps:

**Procedure**

**Step 1** Click **Administration** > **Discovery - LLDP** > **LLDP Neighbor Information**.

**Step 2** Select the interface for which LLDP neighbor information is to be displayed.

This page displays the following fields for the selected interface:

- Local Port—Number of the local port to which the neighbor is connected.
- Chassis ID Subtype—Type of chassis ID (for example, MAC address).
- Chassis ID—Identifier of the 802 LAN neighboring device's chassis.
- Port ID Subtype—Type of the port identifier that is shown.
- Port ID—Identifier of port.
- System Name—Published name of the device.
- Time to Live—Time interval (in seconds) after which the information for this neighbor is deleted.

**Step 3** Select a local port, and click **Details**.

The LLDP Neighbor Information page contains the following fields:

**Port Details**

- Local Port—Port number.

- MSAP Entry—Device Media Service Access Point (MSAP) entry number.

**Basic Details**

- Chassis ID Subtype—Type of chassis ID (for example, MAC address).
- Chassis ID—Identifier of the 802 LAN neighboring device chassis.
- Port ID Subtype—Type of the port identifier that is shown.
- Port ID—Identifier of port.
- Port Description—Information about the port, including manufacturer, product name and hardware/software version.
- System Name—Name of system that is published.
- System Description—Description of the network entity (in alpha-numeric format). This includes the system name and versions of the hardware, operating system, and networking software supported by the device. The value equals the sysDescr object.
- Supported System Capabilities—Primary functions of the device. The capabilities are indicated by two octets. Bits 0 through 7 indicate Other, Repeater, Bridge, WLAN AP, Router, Telephone, DOCSIS cable device, and station, respectively. Bits 8 through 15 are reserved.
- Enabled System Capabilities—Primary enabled function(s) of the device.

**Management Address Table**

- Address Subtype—Managed address subtype; for example, MAC or IPv4.
- Address—Managed address.
- Interface Subtype—Port subtype.
- Interface Number—Port number.

**MAC/PHY Details**

- Auto-Negotiation Supported—Port speed auto-negotiation support status. The possible values are True and False.
- Auto-Negotiation Enabled—Port speed auto-negotiation active status. The possible values are True and False.
- Auto-Negotiation Advertised Capabilities—Port speed auto-negotiation capabilities, for example, 1000BASE-T half duplex mode, 100BASE-TX full duplex mode.
- Operational MAU Type—Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network; for example, 100BASE-TX full duplex mode.

**802.3 Power via MDI**

- MDI Power Support Port Class—Advertised power support port class.
- PSE MDI Power Support—Indicates if MDI power is supported on the port.
- PSE MDI Power State—Indicates if MDI power is enabled on the port.
- PSE Power Pair Control Ability—Indicates if power pair control is supported on the port.
- PSE Power Pair—Power pair control type supported on the port.

- PSE Power Class—Advertised power class of the port.
- Power Type—Type of pod device connected to the port.
- Power Source— Port power source.
- Power Priority—Port power priority.
- PD Requested Power Value—Amount of power requested by the pod device.
- PSE Allocated Power Value—Amount of power allocated by the PSE to the PD.

**4-Wire Power via MDI**

- 4-Pair PoE Supported—Indicates system and port support enabling the 4-pair wire (true only for specific ports that have this HW ability).
- Spare Pair Detection/Classification Required—Indicates that the 4-pair wire is needed.
- PD Spare Pair Desired State—Indicates a pod device requesting to enable the 4-pair ability.
- PD Spare Pair Operational State—Indicates if the 4-pair ability is enabled or disabled.

**802.3 Details**

- 802.3 Maximum Frame Size—Advertised maximum frame size that is supported on the port.

**802.3 Link Aggregation**

- Aggregation Capability—Indicates if the port can be aggregated.
- Aggregation Status—Indicates if the port is currently aggregated.
- Aggregation Port ID—Advertised aggregated port ID.

**802.3 Energy Efficient Ethernet (EEE)**

- Remote Tx—Indicates the time (in micro seconds) that the transmitting link partner waits before it starts transmitting data after leaving Low Power Idle (LPI mode).
- Remote Rx—Indicates the time (in micro seconds) that the receiving link partner requests that the transmitting link partner waits before transmission of data following Low Power Idle (LPI mode).
- Local Tx Echo—Indicates the local link partner’s reflection of the remote link partner’s Tx value.
- Local Rx Echo—Indicates the local link partner’s reflection of the remote link partner’s Rx value.

**MED Details**

- Capabilities Supported—MED capabilities enabled on the port.
- Current Capabilities—MED TLVs advertised by the port.
- Device Class—LLDP-MED endpoint device class. The possible device classes are:
    - Endpoint Class 1—Indicates a generic endpoint class, offering basic LLDP services.
    - Endpoint Class 2—Indicates a media endpoint class, offering media streaming capabilities as well as all Class 1 features.

- Endpoint Class 3—Indicates a communications device class, offering all Class 1 and Class 2 features plus location, 911, Layer 2 switch support and device information management capabilities.

- PoE Device Type—Port PoE type, for example, PD/PSE.
- PoE Power Source—Port's power source.
- PoE Power Priority—Port's power priority.
- PoE Power Value—Port's power value.
- Hardware Revision –Hardware version.
- Firmware Revision—Firmware version.
- Software Revision—Software version.
- Serial Number—Device serial number.
- Manufacturer Name—Device manufacturer name.
- Model Name—Device model name.
- Asset ID—Asset ID.

**802.1 VLAN and Protocol**

- PVID—Advertised port VLAN ID.

**PPVID Table**

- VID—Protocol VLAN ID.
- Supported—Supported Port and Protocol VLAN IDs.
- Enabled—Enabled Port and Protocol VLAN IDs.

**VLAN ID Table**

- VID—Port and Protocol VLAN ID.
- VLAN Name—Advertised VLAN names.

**Protocol ID Table**

- Protocol ID—Advertised protocol IDs.

**Location Information**

Enter the following data structures in hexadecimal as described in section 10.2.4 of the ANSI-TIA-1057 standard:

- Civic—Civic or street address.
- Coordinates—Location map coordinates—latitude, longitude, and altitude.
- ECS ELIN—Device's Emergency Call Service (ECS) Emergency Location Identification Number (ELIN).
- Unknown—Unknown location information.

**Network Policy Table**

- Application Type—Network policy application type, for example, Voice.
- VLAN ID—VLAN ID for which the network policy is defined.
- VLAN Type—VLAN type, Tagged or Untagged, for which the network policy is defined.
- User Priority—Network policy user priority.
- DSCP—Network policy DSCP.

**Step 4** To filter the data in the LLDP Neighbor Table, check **Filter** and select the local port from the drop-down list. Then, click **Go** to display the chosen port.

**Step 5** To delete a port from the LLDP Neighbor Table, select the port and click the delete icon.

# LLDP Statistics

The LLDP Statistics page displays LLDP statistical information per port.

To view the LLDP statistics, follow these steps:

### Procedure

**Step 1** Click **Administration** > **Discovery - LLDP** > **LLDP Statistics**.

For each port, the fields are displayed:

- Interface—Identifier of interface.
- Tx Frames (Total)—Number of transmitted frames.
- Rx Frames
  - Total—Number of received frames
  - Discarded—Total number of received frames that discarded
  - Errors—Total number of received frames with errors
- Rx TLVs
  - Discarded—Total number of received TLVs that discarded
  - Unrecognized—Total number of received TLVs that unrecognized.
- Neighbor's Information Deletion Count—Number of neighbor ageouts on the interface.

**Step 2** Click **Refresh** to view the latest statistics.

# LLDP Overloading

**Note** This setting is only available in the Advanced Mode view.)

LLDP adds information as LLDP and LLDP-MED TLVs into the LLDP packets. LLDP overload occurs when the total amount of information to be included in an LLDP packet exceeds the maximum PDU size supported by an interface.

The LLDP Overloading page displays the number of bytes of LLDP/LLDP-MED information, the number of available bytes, and the overloading status of every interface.

To view LLDP overloading information:

### Procedure

**Step 1** Click **Administration** > **Discovery - LLDP** > **LLDP Overloading**.

In the LLDP Overloading Table, the following information is displayed for each port:

- Interface—Port identifier.
- Total Bytes In-Use—Total number of bytes of LLDP information in each packet
- Available Bytes Left—Total amount of available bytes left for other LLDP information in each packet.
- Status—Whether TLVs are being transmitted or if they are overloaded.

**Step 2** To view the overloading details for a port, select it and click **Details**.

This page contains the following information for each TLV sent on the port:

- Interface—Select the interface from the drop-down list.
- LLDP Mandatory TLVs
  - Size (Bytes)—Total mandatory TLV byte size
  - Status—If the mandatory TLV group is being transmitted, or if the TLV group was overloaded.
- LLDP MED Capabilities
  - Size (Bytes)—Total LLDP MED capabilities packets byte size
  - Status—If the LLDP MED capabilities packets sent, or if they overloaded.
- LLDP MED Location
  - Size (Bytes)—Total LLDP MED location packets byte size
  - Status—If the LLDP MED locations packets sent, or if they overloaded.
- LLDP MED Network Policy
  - Size (Bytes)—Total LLDP MED network policies packets byte size

- Status—If the LLDP MED network policies packets sent, or if they overloaded.

- LLDP MED Extended Power via MDI
  - Size (Bytes)—Total LLDP MED extended power via MDI packets byte size.
  - Status—If the LLDP MED extended power via MDI packets sent, or if they overloaded.

- 802.1 TLVs
  - Size (Bytes)—Total LLDP MED 802.1 TLVs packets byte size.
  - Status—If the LLDP MED 802.1 TLVs packets sent, or if they overloaded.

- 802.3 TLVs
  - Size (Bytes)—Total LLDP MED 802.3 TLVs packets byte size.
  - Status—If the LLDP MED 802.3 TLVs packets sent, or if they overloaded.

- LLDP Optional TLVs
  - Size (Bytes)—Total LLDP MED optional TLVs packets byte size.
  - Status—If the LLDP MED optional TLVs packets sent, or if they overloaded.

- LLDP MED Inventory
  - Size (Bytes)—Total LLDP MED inventory TLVs packets byte size.
  - Status—If the LLDP MED inventory packets sent, or if they overloaded.

- Total
  - Total (Bytes)—Total number of bytes of LLDP information in each packet.
  - Available Bytes Left—Total number of available bytes left to send for additional LLDP information in each packet.

# Discovery - CDP

Cisco Discovery Protocol is a Layer 2, media-independent, and network-independent protocol that networking applications use to learn about nearby, directly connected devices. Cisco Discovery Protocol is enabled by default. Each device configured for Cisco Discovery Protocol advertises at least one address at which the device can receive messages and sends periodic advertisements (messages) to the well-known multicast address 01:00:0C:CC:CC:CC. Devices discover each other by listening at that address. They also listen to messages to learn when interfaces on other devices are up or go down.

Advertisements contain time-to-live information, which indicates the length of time a receiving device should hold Cisco Discovery Protocol information before discarding it. Advertisements supported and configured in Cisco software are sent, by default, every 60 seconds on interfaces that support Subnetwork Access Protocol (SNAP) headers. Cisco devices never forward Cisco Discovery Protocol packets. Cisco devices that support

Cisco Discovery Protocol store the information received in a table. Information in this table is refreshed every time an advertisement is received, and information about a device is discarded after three advertisements from that device are missed.

This section describes how to configure CDP.

# Properties

Similar to LLDP, the Cisco Discovery Protocol (CDP) is a link layer protocol for directly connected neighbors to advertise themselves and their capabilities to each other. Unlike LLDP, CDP is a Cisco proprietary protocol. To configure the CDP properties, complete the following steps:

### Procedure

**Step 1** Click **Administration** > **Discovery - CDP** > **Properties**.

**Step 2** Enter the parameters.

| | |
|---|---|
| CDP Status | Select to enable CDP on the device. |
| CDP Frames Handling | If CDP is not enabled, select the action to be taken if a packet that matches the selected criteria is received:<br>• Bridging—Forward the packet based on the VLAN<br>• Filtering—Delete the packet<br>• Flooding—VLAN unaware flooding that forwards incoming CDP packets to all the ports excluding the ingress ports. |
| CDP Voice VLAN Advertisement | Select to enable the device to advertise the voice VLAN in CDP on all of the ports that are CDP enabled, and are member of the voice VLAN. The voice VLAN is configured in the Properties. |
| CDP Mandatory TLVs Validation | If selected, incoming CDP packets not containing the mandatory TLVs are discarded and the invalid error counter is incremented. |
| CDP Version | Select the version of CDP to use. |
| CDP Hold Time | Amount of time that CDP packets are held before the packets are discarded, measured in multiples of the TLV Advertise Interval. For example, if the TLV Advertise Interval is 30 seconds, and the Hold Multiplier is 4, then the LLDP packets are discarded after 120 seconds. The following options are possible:<br>• Use Default—Use the default time (180 seconds)<br>• User Defined—Enter the time in seconds. |
| CDP Transmission Rate | The rate in seconds at which CDP advertisement updates are sent. The following options are possible:<br>• Use Default—Use the default rate (60 seconds)<br>• User Defined—Enter the rate in seconds. |

| | |
|---|---|
| Device ID Format | Select the format of the device ID (MAC address or serial number). The following options are possible:<br>• Mac Address—Use the MAC address of the device as the device ID.<br>• Serial Number—Use the serial number of the device as the device ID.<br>• Hostname—Use the host name of the device as the device ID. |
| Source Interface | IP address to be used in the TLV of the frames. The following options are possible:<br>• Use Default—Use the IP address of the outgoing interface.<br>• User Defined—Use the IP address of the interface (in the Interface field) in the address TLV. |
| Interface | IF User Defined was selected for Source Interface, select the interface. |
| Syslog Voice VLAN Mismatch | Check to send a SYSLOG message when a voice VLAN mismatch is detected. This means that the voice VLAN information in the incoming frame does not match what the local device is advertising. |
| Syslog Native VLAN Mismatch | Check to send a SYSLOG message when a native VLAN mismatch is detected. This means that the native VLAN information in the incoming frame does not match what the local device is advertising. |
| Syslog Duplex Mismatch | Check to send a SYSLOG message when duplex information is mismatched. This means that the duplex information in the incoming frame does not match what the local device is advertising. |

**Step 3** Click **Apply**. The LLDP properties are defined.

# Interface Settings

**Note** This setting is only available in the Advanced Mode view.

The Interface Settings page enables you to enable/disable CDP per port. By setting these properties, it's possible to select the types of information to be provided to devices that support the LLDP protocol.

The LLDP-MED TLVs to be advertised can be selected in the LLDP MED Port Settings, on page 42.

To define the CDP interface settings:

**Procedure**

**Step 1** Click **Administration** > **Discovery - CDP** > **Interface Settings**.

This page displays the following CDP information for each interface.

- Entry No. — CDP entry.
- Interface —Interface used for CDP entry.
- CDP Status—CDP publishing option for the port.
- Reporting Conflicts with CDP Neighbors—Status of the reporting options that are enabled/disabled in the Edit page (Voice VLAN/Native VLAN/Duplex).
- No. of Neighbors—Number of neighbors detected.

The bottom of the page has four buttons:

- Copy Settings—Select to copy a configuration from one port to another.
- Edit—Fields explained in Step 2 below.
- CDP Local Information Details—Takes you to the CDP Local Information, on page 56 .
- CDP Neighbor Information Details—Takes you to the CDP Neighbors Information, on page 58.

**Step 2** Select a port and click **Edit.**

This page provides the following fields:

- Interface—Select the interface to be defined.
- CDP Status—Select to enable/disable the CDP publishing option for the port.

**Note**
The next three fields are operational when the device has been set up to send traps to the management station.

- Syslog Voice VLAN Mismatch—Select to enable sending a SYSLOG message when a voice VLAN mismatch is detected. This means that the voice VLAN information in the incoming frame doesn't match what the local device is advertising.
- Syslog Native VLAN Mismatch—Select to enable sending a SYSLOG message when a native VLAN mismatch is detected. This means that the native VLAN information in the incoming frame doesn't match what the local device is advertising.
- Syslog Duplex Mismatch—Select to enable sending a SYSLOG message when duplex information mismatch is detected. This means that the duplex information in the incoming frame doesn't match what the local device is advertising.

**Step 3** Enter the relevant information, and click **Apply**. The port settings are written to the Running Configuration.

# CDP Local Information

To view information that is advertised by the CDP protocol about the local device:

### Procedure

Click **Administration** > **Discovery - CDP** > **CDP Local Information**. The following fields are displayed:

| | |
|---|---|
| Interface | Number of the local port. |
| CDP State | Displays whether CDP is enabled or not. |
| Device ID TLV | • Device ID Type—Type of the device ID advertised in the device ID TLV<br>• Device ID—Device ID advertised in the device ID TLV |
| System Name TLV | System Name—System name of the device. |
| Address TLV | Address1-3—IP addresses (advertised in the device address TLV). |
| Port TLV | Port ID—Identifier of port advertised in the port TLV. |
| Capabilities TLV | Capabilities—Capabilities advertised in the port TLV). |
| Version TLV | Version—Information about the software release on which the device is running. |
| Platform TLV | Platform—Identifier of platform advertised in the platform TLV. |
| Native VLAN TLV | Native VLAN—The native VLAN identifier advertised in the native VLAN TLV. |
| Full/Half Duplex TLV | Duplex—Whether port is half or full-duplex advertised in the full/half duplex TLV. |
| Appliance TLV | • Appliance ID—Type of device attached to port advertised in the appliance TLV<br>• Appliance VLAN ID—VLAN on the device used by the appliance, for instance if the appliance is an IP phone, this is the voice VLAN. |
| Extended Trust TLV | Extended Trust—Enabled indicates that the port is trusted, and the packets received are marked. In this case, packets received on such a port aren't re-marked. Disabled indicates that the port isn't trusted in which case, the following field is relevant. |
| CoS for Untrusted Ports TLV | CoS for Untrusted Ports—If Extended Trust is disabled on the port, this field displays the Layer 2 CoS value, meaning, an 802.1D/802.1p priority value. This is the COS value with which all packets received on an untrusted port are remarked by the device. |
| Power Available TLV | • Request ID—Last power request ID received echoes the Request-ID field last received in a Power Requested TLV. It's 0 if no Power Requested TLV was received since the interface last transitioned to Up.<br>• Power Management ID—Value incremented by 1 (or 2, to avoid 0) each time any one of the following events occurs:<br>Available-Power or Management Power Level change<br>A Power Requested TLV is received with a Request-ID that is different from the last-received set.<br>The interface transitions to Down.<br>• Available Power—Amount of power consumed by port<br>• Management Power Level—Displays the supplier's request to the pod device for its Power Consumption TLV. The device always displays "No Preference" in this field. |

| | |
|---|---|
| 4-Wire Power via MDI (UPOE) TLV | Displays whether this TLV is supported.<br>• 4-Pair PoE Supported—Displays whether PoE is supported.<br>• Spare Pair Detection/Classification Required—Displays whether this classification is required.<br>• PD Spare Pair Desired State—Displays the PD spare pair desired state.<br>• PD Spare Pair Operational State—Displays the PSE spare pair state. |

# CDP Neighbors Information

The CDP Neighbors Information page displays CDP information received from neighboring devices.

Information is deleted, after timeout (based on the value received from Time To Live TLV during which no CDP PDU was received).

To view the CDP neighbors information, proceed as follows:

### Procedure

**Step 1** Click **Administration** > **Discovery - CDP** > **CDP Neighbor Information**.

**Step 2** To start a new instance, click **Clear Table** to clear out the previous data in the CDP Neighbor Information Table.

**Step 3** To select a filter, check the Filter checkbox, select a Local interface, and click **Go**.

The filter is applied on the list, and Clear Filter is activated to enable stopping the filter.

The CDP Neighbor Information page contains the following fields for the link partner (neighbor):

| | |
|---|---|
| Device ID | Neighbors device ID. |
| System Name | Neighbors system name. |
| Local Interface | Number of the local port to which the neighbor is connected. |
| Advertisement Version | CDP protocol version. |
| Time to Live (sec) | Time interval (in seconds) after which the information for this neighbor is deleted. |
| Capabilities | Capabilities advertised by neighbor. |
| Platform | Information from Platform TLV of neighbor. |
| Neighbor Interface | Outgoing interface of the neighbor. |

**Step 4** Select a device, and click **Details**.

This page contains the following fields about the neighbor (actual field display depends on what the neighbor is advertising):

| | |
|---|---|
| Device ID | Neighbors device ID. |

| | |
|---|---|
| System Name | Neighbors system name. |
| Local Interface | Number of the local port to which the neighbor is connected. |
| Advertisement Version | CDP protocol version. |
| Time to Live | Time interval (in seconds) after which the information for this neighbor is deleted. |
| Capabilities | Capabilities advertised by neighbor. |
| Platform | Information from Platform TLV of neighbor. |
| Neighbor Interface | Outgoing interface of the neighbor. |
| Native VLAN | Neighbors native VLAN. |
| Application | Neighbors application, |
| Duplex | Whether neighbors interface is half or full-duplex. |
| Addresses | Neighbors addresses. |
| Power Drawn | Amount of power consumed by neighbor on the interface. |
| Version | Neighbors software version. |
| Power Request | Power requested by PD that is connected to the port.<br>• Power Request List—Each PD may send a list (up to 3) of supported power levels. |
| 4-Wire Power via MDI | • 4-Pair PoE Supported—Indicates system and port support enabling the 4-pair wire.<br>• Spare Pair Detection/Classification Required—Indicates that the 4-pair wire is needed.<br>• PD Spare Pair Desired State—Indicates a pod device requesting to enable the 4-pair ability.<br>• PD Spare Pair Operational State—Indicates whether the 4-pair ability is enabled or disabled. |

**Note** Disconnects on the Clear Table button all connected devices if from CDP, and if Auto Smartport is enabled change all port types to default.

# CDP Statistics

The CDP Statistics page displays information regarding CDP frames that sent or received from a port. CDP packets are received from devices attached to the switches interfaces, and are used for the Smartport feature.

To view CDP statistics, follow these steps:

### Procedure

**Step 1** Click **Administration** > **Discovery - CDP** > **CDP Statistics.**

The following fields are displayed for every interface:

Packets Received/Packets Transmitted:

- Version 1—Number of CDP version 1 packets received/transmitted.
- Version 2—Number of CDP version 2 packets received/transmitted.
- Total—Total number of CDP packets received/transmitted.

CDP Error Statistics:

- Illegal Checksum—Number of packets received with illegal checksum value.
- Other Errors—Number of packets received with errors other than illegal checksums.
- Neighbors Over Maximum—Number of times that packet information couldn't be stored in cache because of lack of room.

**Step 2** To clear all counters on all interfaces, click **Clear All Interface Counters**. To clear all counters on an interface, select it and click **Clear Interface Counters**.

# Locate Device

This feature enables flashing all network port LEDs on a specific device in the network to locate the device physically. This feature is useful for locating a device within a room with many interconnected devices. When this feature is activated, all network port LEDs on the device flash for a configured duration (one minute by default).

### Procedure

**Step 1** Click **Administration** > **Locate Device**.

**Step 2** Enter values in the following fields:

- Duration—Enter for how long (in seconds) the port's LEDs flash.
- Remaining Time—This field is only displayed if the feature is currently activated. It displays the remaining time during which the LED flashes.
- Unit ID—This field is only displayed when the device is in a stack. Specify the unit on which the network port LEDs flash or All for all units.

**Step 3** Click **Start** to activate the feature.

When the feature is activated the Start button is replaced by the Stop button, which allows you to stop the LED blinking before the defined timer expires.

# Ping

The Ping utility tests if a remote host can be reached and measures the round-trip time for packets sent.

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response, sometimes called a pong. It measures the round-trip time and records any packet loss.

To ping a host, follow these steps:

### Procedure

**Step 1** Click **Administration** > **Ping**.

**Step 2** Configure ping by entering the fields:

| Option | Description |
|---|---|
| Host Definition | Select whether to specify the source interface by its IP address or name. This field influences the interfaces that are displayed in the Source IP field, as described below. |
| IP Version | If the source interface is identified by its IP address, select either IPv4 or IPv6 to indicate that it will be entered in the selected format. |
| Source IP | Select the source interface as the source IPv4 address for communication with the destination. If the Host Definition field was By Name, all IPv4 and IPv6 addresses are displayed. If the Host Definition field was By IP Address, only the existing IP addresses of the type specified in the IP Version field are displayed.<br>**Note**<br>If the Auto option is selected, the system computes the source address based on the destination address. |
| Destination IPv6 Address Type | Select one of the following options:<br>• 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.<br>• 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 from where it is received. |

| Option | Description |
|---|---|
| Destination IP Address/Name | Address or host name of the device to be pinged. Whether this is an IP address or host name depends on the Host Definition. |
| Ping Interval<br>**Note**<br>This setting is only available in the Advanced Mode view. | Length of time the system waits between ping packets. Ping is repeated the number of times configured in the Number of Pings fields, whether the ping succeeds or not. Select to use the default interval or specify your own value. |
| Number of Pings<br>**Note**<br>This setting is only available in the Advanced Mode view. | The number of times the ping operation is performed. Select to use the default or specify your own value. |
| Status | Displays whether the ping succeeded or failed. |

**Step 3** Click **Activate Ping** to ping the host. The ping status appears and a message is added to the list of messages, indicating the result of the ping operation.

**Step 4** View the results of ping in the Ping Counters and Status section of the page:

- Number of Sent Packets—Number of packets sent by ping
- Number of Received Packets—Number of packets received by ping
- Packet Loss—Percentage of packets lost in ping process
- Minimum Round Trip Time—Shortest time for packet to return
- Maximum Round Trip Time—Longest time for packet to return
- Average Round Trip Time—Average time for packet to return
- Status—Fail or succeed

# Traceroute

Traceroute discovers the IP routes forwarded by sending an IP packet to the target host and back to the device. The Traceroute page shows each hop between the device and a target host, and the round-trip time to each such hop.

### Procedure

**Step 1** Click **Administration** > **Traceroute**.

**Step 2** Configure Traceroute by entering information in the following fields:

- Host Definition—Select whether hosts are identified by their IP address or name.

- IP Version—If the host is identified by its IP address, select either IPv4 or IPv6 to indicate that it will be entered in the selected format.
- Source IP—Select the source interface whose IPv4 address will be used as the source IPv4 address for communication messages. If the Host Definition field was By Name, all IPv4 and IPv6 addresses are displayed in this drop-down field. If the Host Definition field was By IP Address, only the existing IP addresses of the type specified in the IP Version field will be displayed.
- Host IP Address/Name—Enter the host address or name.
- TTL—Enter the maximum number of hops that Traceroute permits. This is used to prevent a case where the sent frame gets into an endless loop. The Traceroute command terminates when the destination is reached or when this value is reached. To use the default value (30), select **Use Default**.

  **Note**
  This setting is only available in the Advanced Mode view.

- Timeout—Enter the length of time that the system waits for a frame to return before declaring it lost, or select **Use Default**.

  **Note**
  This setting is only available in the Advanced Mode view.

**Step 3** Click **Activate Traceroute**. The operation is performed.

**Note**
A pop-up will appear indicating if you would like to stop the traceroute. Click **Stop Traceroute** to stop the process.

A page appears to show the Round Trip Time (RTT) and status for each trip in the fields:

- Index—Displays the number of the hop.
- Host—Displays a stop along the route to the destination.

  Round Trip Time (1-3)—Displays the round trip Time (ms) and Status.