Port Management

This chapter contains the following sections:

Port Settings

The Port Settings page displays the global and per-ports settings of all the ports. Here, you can select and configure the needed ports from the Edit Port Settings page.

To configure port settings, follow these steps:

Procedure

Step 1 Click **Port Management** > **Port Settings**.

The port settings are displayed for all ports.

Step 2 Configure the following options:

- Link Flap Prevention—Select to minimize the disruption to your network. Enabled (default), this command automatically disables ports that experience link-flap events.
- Jumbo Frames—Check to support packets of up to 9 KB in size. If Jumbo Frames isn't enabled (default), the system supports a packet size up to 2,000 bytes. Receiving packets bigger than 9 KB might cause the receiving port to shut down. Also, sending packets bigger than 10 KB bytes might cause the receiving port to shut down.

  For jumbo frames to take effect, the device must be rebooted after the feature is enabled.

Step 3 Click **Apply** to update the global setting.

Jumbo frames configuration changes take effect only after the Running Configuration is explicitly saved to the Startup Configuration File using the File Operations, and the device is rebooted.

Step 4 To update the port settings, select the needed port, and click **Edit.**

Step 5 Modify the following parameters:

Interface	Select the port number.
Port Description	Enter the port user-defined name or comment. **Note** The Interface and Port Description are displayed on the main page in the Port column.
Port Type	Displays the port type and speed. The possible options are: • Copper Ports—Regular, not Combo, support the following values: 10M, 100M, 1000M, 2500M (type: Copper) and 10G. • Combo Ports—Combo port that is connected with either copper CAT6a cable or SFP Fiber Gigabit Interface • 10G-Fiber Optics—Ports with speed of either 1G or 10G
Administrative Status	Select whether the port must be Up or Down when the device is rebooted. This also occurs after clicking the apply button. So the port will be up or down after making the selection and clicking apply in addition to the port after a reboot.
Operational Status	Displays whether the port is currently Up or Down. If the port is down because of an error, the description of the error is displayed
Link Status SNMP Traps	Select to enable generation of SNMP traps that notify of changes to the link status of the port.
Time Range	Select to enable the time range during which the port is in Up state. When the time range isn't active, the port is in shutdown. If a time range is configured, it's effective only when the port is administratively Up.
Time Range Name	Select the profile that specifies the time range. Not relevant for the OOB port. If a time range isn't yet defined, click **Edit**.
Operational Time Range State	Range State—Displays whether the time range is currently active or inactive.
Auto Negotiation	Select to enable auto-negotiation on the port. Auto-negotiation enables a port to advertise its transmission speed, duplex mode to the port link partner.
Operational Auto Negotiation	Displays the current auto-negotiation status on the port.
Administrative Port Speed	Select the speed of the port. The port type determines the available speeds. You can designate Administrative Speed only when port auto-negotiation is disabled.
Operational Port Speed	Displays the current port speed that is the result of negotiation.

Administrative Duplex Mode	Select from one of the following options: • Full - Allows the interface to transmit data between the switch and the client in both directions at the same time. • Half - Allows the interface to transmit data between the switch and the client in one direction at a time.
Operational Duplex Mode	Displays the current duplex mode for a port.
Auto Advertisement	Select the capabilities advertised by auto-negotiation when it's enabled. **Note** Not all options are relevant for all devices. The options are: • Max Capability—All port speeds and duplex mode settings can be accepted. • 10 Half—10-Mbps speed and Half Duplex mode (doesn't appear on XG devices) • 10 Full—10-Mbps speed and Full Duplex mode (doesn't appear on XG devices) • 100 Half—100-Mbps speed and Half Duplex mode (doesn't appear on XG devices) • 1000 Full—1000-Mbps speed and Full Duplex mode • 2500 Full—2500-Mbps speed and Full Duplex mode • 5000 Full—5000-Mbps speed and Full Duplex mode • 10000 Full—10,000-Mbps speed and Full Duplex mode
Operational Advertisement	Displays the capabilities that are currently published to the ports neighbor. The possible options are those specified in the Administrative Advertisement field.
Preference Mode	Available only if auto-negotiation is enabled. Select the active-member mode of the interface for the auto-negotiation operation. Select one of the following options: • Slave—Begin negotiation with the preference that the device port is the member in the auto-negotiation process. • Master—Begin negotiation with the preference that the device port is the active in the auto-negotiation process.
Neighbor Advertisement	Displays the capabilities that are advertised by the neighboring device.
Back Pressure	Select the Back Pressure mode on the port (used with Half Duplex mode) to slow down the packet reception speed when the device is congested. Selecting this option disables the remote port, preventing it from sending packets by jamming the signal.
Flow Control	Enable or disable 802.3x Flow Control on the port (only when in Full Duplex mode).

MDI/MDIX-Media Dependent Interface (MDI)/Media Dependent Interface with Crossover (MDIX) status on the port.	The options are: • MDIX—Select to swap the port's transmit and receive pairs. • MDI—Select to connect this device to a station by using a straight-through cable. • Auto-Select to configure this device to automatically detect the correct pinouts for connection to another device.
Operational MDI/MDIX	Displays the current MDI/MDIX setting.
Protected Port	Select to make this protected port. (A protected port is also referred as a Private VLAN Edge (PVE).) The features of a protected port are as follows: • Protected Ports provide Layer 2 isolation between interfaces (Ethernet ports and LAGs) that share the same VLAN. • Packets that are received from protected port scan be forwarded only to unprotected egress ports. Protected port filtering rules are also applied to packets that are forwarded by software, such as snooping applications. • Port protection isn't subject to VLAN membership. Devices connected to protected ports aren't allowed to communicate with each other, even if they are members of the same VLAN. • Both ports and LAGs can be defined as protected or unprotected. Protected LAGs are described in LAG Settings, on page 7.
Member in LAG	If the port is a member of a LAG, the LAG number appears; otherwise this field is left blank.

Step 6 Click **Apply**. The Port Settings are written to the Running Configuration file.

Error Recovery Settings

The Error Recovery Settings page enables the user to automatically reactivate a port that has been shut down because of a device error that occurs after the Automatic Recovery Interval has passed.

To configure the error recovery settings, complete these steps:

Procedure

Step 1 Click **Port Management** > **Error Recovery Settings**.

Step 2 Enter the following fields:

- Automatic Recovery Interval—Specify the time delay for automatic error recovery, if enabled, after a port is shut down.
- Automatic ErrDisable Recovery

- Port Security—Select to enable automatic error recovery when the port is shut down for port security violations.
- 802.1x Single Host Violation—Select to enable automatic error recovery when the port is shut down by 802.1x.
- ACL Deny—Select to enable automatic error recovery mechanism by an ACL action.
- STP Loopback Guard—Enable automatic recovery when the port is shut down by STP Loopback Guard.
- Loopback Detection—Select to enable error recovery mechanism for ports shut down by loopback detection.
- Storm Control—Select to enable error recovery mechanism for ports shut down by storm control.
- Link Flap Prevention—Select to enable error recovery mechanism for ports shut down by link flap prevention.

Step 3 Click **Apply** to update the global setting.

To manually reactivate a port follow these steps:

Step 4 Click **Port Management** > **Error Recovery Settings**.

The list of inactivated interfaces along with their Suspension Reason is displayed in the Suspended (errDisabled) Interface Table.

Step 5 To filter the Suspension Reason, select a reason and click **Go**. Then, only the interfaces that are suspended for that reason are displayed in the table.

Step 6 Select the interface to be reactivated.

Step 7 Click **Reactivate**.

Loopback Detection Settings

Loopback Detection (LBD) provides protection against loops by transmitting loop protocol packets out of ports on which loop protection has been enabled. When the switch sends out a loop protocol packet, and then receives the same packet, it shuts down the port that received the packet.

Loopback Detection operates independently of STP. After a loop is discovered, the port that received the loops is placed in the Shut Down state. A trap is sent and the event is logged. Network managers can define a Detection Interval that sets the time interval between LBD packets.

To enable and configure LBD, follow these steps:

Procedure

Step 1 Click **Port Management** > **Loopback Detection Settings**.

Step 2 Select **Enable** in the Loopback Detection to enable the feature.

Step 3 Enter the Detection Interval. This is the interval between transmission of LBD packets. (Range 5-60, Default 30).

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

The following fields are displayed for each interface, regarding the Loopback Detection State:

- Administrative—Loopback detection is enabled.

- Operational—Loopback detection is enabled but not active on the interface.

Step 5 Select whether to enable LBD on ports or LAGS in the Interface Type equals field in the filter.

Step 6 Select the ports or LAGs on which LBD is to be enabled and click **Edit**.

Step 7 Select the settings for the chosen Interface. Next, check **Enable** in the Loopback Detection State field for the port or LAG selected.

Step 8 Click **Apply** to save the configuration to the Running Configuration file.

Link Aggregation

Link aggregation applies to various methods of combining multiple network connections in parallel in order to increase throughput beyond what a single connection could sustain. It provides redundancy in case one of the links should fail.

Link Aggregation Control Protocol (LACP) is part of the IEEE specification (802.3ad) that enables you to bundle several ports together to form a single logical channel (LAG). LAGs multiply bandwidth, increase port flexibility, and provide link redundancy between two devices.

Two types of LAGs are supported:

- Static—The ports in the LAG are manually configured. A LAG is static if LACP is disabled on it. The group of ports assigned to a static LAG are always active members. After a LAG is manually created, the LACP option can't be added or removed, until the LAG is edited and a member is removed (which can be added back prior to applying); the LACP button then become available for editing.
- Dynamic—A LAG is dynamic if LACP is enabled on it. The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports. The nonactive candidate ports are standby ports ready to replace any failing active member ports.

This section describes how to configure LAGs.

LAG Management

Link Aggregation Control Protocol (LACP) is part of the IEEE specification (802.3ad) that enables you to bundle several ports together to form a single logical channel (LAG). LAGs multiply bandwidth, increase port flexibility, and provide link redundancy between two devices.

To select the load-balancing algorithm of the LAG, follow these steps:

Procedure

Step 1 Click **Port Management** > **Link Aggregation** > **LAG Management.**

Step 2 Select one of the following Load Balance Algorithm:

- MAC Address—Perform load balancing by source and destination MAC addresses on all packets.
- IP/MAC Address—Perform load balancing by the IP addresses on the IP packets, and by MAC addresses on non-IP packets

Step 3 Click **Apply**. The Load Balance Algorithm is saved to the Running Configuration file.

To define the member or candidate ports in a LAG.

Step 4 Select the LAG to be configured, and click **Edit.**

Step 5 Enter the values for the following fields:

- LAG—Select the LAG number.
- LAG Name—Enter the LAG name or a comment.
- LACP—Select to enable LACP on the selected LAG. This makes it a dynamic LAG. This field can only be enabled after moving a port to the LAG in the next field.
- Port List—Move the ports that are assigned to the Port List LAGs to the LAG Members. Up to eight ports per static LAG can be assigned, and 16 ports can be assigned to a dynamic LAG.

Step 6 Click **Apply**. LAG membership is saved to the Running Configuration file.

LAG Settings

The LAG Settings page displays a table of current settings for all LAGs. You can configure the settings of selected LAGs, and reactivate suspended LAGs by launching the Edit LAG Settings page.

To configure the LAG settings or reactivate a suspended LAG:

Procedure

Step 1 Click **Port Management** > **Link Aggregation** > **LAG Settings**.

The LAGs in the system are displayed.

Step 2 Select a LAG, and click **Edit**.

Step 3 Enter the values for the following fields:

Option	Description
LAG	Select the LAG ID number.
LAG Type	Displays the port type that comprises the LAG.
Description	Enter the LAG name or a comment.
Administrative Status	Set the selected LAG to be Up or Down.
Link Status SNMP Traps	Select to enable generation of SNMP traps notifying of changes to the link status of the ports in the LAG.
Time Range	Check Enable to enable time range during which the port is in Up state. When the time range is not active, the port is in shutdown. If a time range is configured, it is effective only when the port is administratively up.

Option	Description
Time Range Name	Select the profile that specifies the time range. If a time range is not yet defined, click **Edit** to configure the time range.
Operational Status	Displays whether the LAG is currently operating.
Operational Time Range State	Displays whether the time range is currently active or inactive.
Administrative Auto Negotiation	Enables or disable auto-negotiation on the LAG. Auto-negotiation is a protocol between two link partners that enables a LAG to advertise its transmission speed to its partner. It is recommended to keep auto-negotiation enabled on both sides of an aggregate link, or disabled on both sides, while ensuring that link speeds are identical.
Administrative Speed	Displays the speed of the ports in the LAG.
Administrative Advertisement	Check Max Capability to allow for all LAG speeds and both duplex modes are available. Select the capabilities to be advertised by the LAG. The options are:
Administrative Flow Control	Set Flow Control to either Enable or Disable on the LAG.
Operational Auto Negotiation	Displays the auto-negotiation setting.
Operational LAG Speed	Displays the current speed at which the LAG is operating.
Operational Advertisement	Displays the Administrative Advertisement status. The LAG advertises its capabilities to its neighbor LAG to start the negotiation process. The possible values are those specified in the Administrative Advertisement field.
Operational Flow Control	Displays the current Flow Control setting.

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

LACP

A dynamic LAG is LACP-enabled, and LACP is run on every candidate port defined in the LAG. LACP system priority and LACP port priority are both used to determine which of the candidate ports become active member ports in a dynamic LAG configured with more than eight candidate ports.

Use the LACP page to configure the candidate ports for the LAG and to configure the LACP parameters per port. With all factors equal, when the LAG is configured with more candidate ports than the maximum number of active ports allowed (8), the device selects ports as active from the dynamic LAG on the device that has the highest priority.

Note The LACP setting is irrelevant on ports that are not members of a dynamic LAG.

To define the LACP settings, complete the following steps:

Procedure

Step 1 Click **Port Management** > **Link Aggregation** > **LACP**.

Step 2 If needed, edit the LACP System Priority and click **Apply**.

Step 3 To edit an existing port, select the port, and click **Edit.**

Step 4 In the Edit LACP Settings dialog box, enter the values for the following fields:

- Port—Select the port number to which timeout and priority values are assigned.
- LACP Port Priority—Enter the LACP priority value for the port.
- LACP Timeout—Time interval between the sending and receiving of consecutive LACP PDUs. Select the periodic transmissions of LACP PDUs, which occur at either a Long or Short transmission speed, depending upon the expressed LACP timeout preference.

Step 5 Click **Apply**. The Running Configuration file is updated.

UDLD

UDLD is a Layer 2-protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to detect unidirectional links. A unidirectional link occurs whenever traffic from a neighboring device is received by the local device, but traffic from the local device is not received by the neighbor.

The purpose of UDLD is to detect ports on which the neighbor does not receive traffic from the local device (unidirectional link) and to shut down those ports.

All connected devices must support UDLD for the protocol to successfully detect unidirectional links. If only the local device supports UDLD, it is not possible for the device to detect the status of the link. In this case, the status of the link is set to undetermined. The user can configure whether ports in the undetermined state are shut down or not.

UDLD Global Settings

The Fiber Port UDLD Default State is only applicable to fiber ports.

The Message Time field is applicable to both copper and fiber ports.

To configure UDLD globally, follow these steps:

Procedure

Step 1 Click **Port Management** > **UDLD** > **UDLD Global Settings**.

Step 2 Enter the following fields:

- Message Time—Enter the interval between sending UDLD messages. This field is relevant for both fiber and copper ports.
- Fiber Port UDLD Default State—This field is only relevant for fiber ports. The possible states are:
  - Disabled—UDLD is disabled on all ports of the device.
  - Normal—Device shuts down an interface if the link is unidirectional. If the link is undetermined, a notification is issued.
  - Aggressive—Device shuts down an interface if the link is uni-directional. If the link is bi-directional, the device shuts down after the UDLD information times out. The port state is marked as undetermined.

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

UDLD Interface Settings

Use the UDLD Interface Settings page to change the UDLD state for a specific port. Here the state can be set for copper or fiber ports. To copy a particular set of values to more than one port, set that value for one port and use the Copy button to copy it to the other ports.

To configure UDLD for an interface, follow these steps:

Procedure

Step 1 Click **Port Management** > **UDLD** > **UDLD Interface Settings**.

Information is displayed for all UDLD enabled ports, or a selected group of ports.

- Interface—Select the interface from the drop-down list.
- UDLD State—The possible states are:
  - Default—Port receives the value of the Fiber Port UDLD Default State.
  - Disabled—UDLD is disabled on all fiber ports of the device.
  - Normal—Device shuts down an interface if it detects that the link is unidirectional. It issues a notification if the link is undetermined.
  - Aggressive—Device shuts down an interface if the link is uni-directional. If the link is bi-directional, the device shuts down after the UDLD information times out. The port state is marked as undetermined.
- Bidirectional State—The possible states are:
  - Detection—The latest UDLD state of the port is in the process of being determined. Expiration time won't expire since the last determination (if there was one), or since UDLD began running on the port, so that the state isn’t yet determined.
  - Bidirectional—Traffic sent by the local device is received by its neighbor, and traffic from the neighbor is received by the local device.

- Undetermined—The state of the link between the port and its connected port can't be determined either because no UDLD message was received or the UDLD message didn't contain the local device ID in it.
- Disabled (Default)—UDLD has been disabled on this port.
- Shutdown—The port has been shut down because its link with the connected device is undetermined in aggressive mode.
- Idle—The port is idle.

- Number of Neighbors—Number of connected devices detected.

Step 2 To modify the UDLD state for a specific port, select it and click **Edit**.

Step 3 Modify the value of the UDLD state.

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

UDLD Neighbors

To view all devices connected to the local device, click **Port Management** > **UDLD** > **UDLD Neighbors**.

To filter the fields displayed, add a check mark to **Filter**, enter a value for the **Interface Name** equals to and click **Go**.

The following fields are displayed for all UDLD-enabled ports.

- Interface Name—Name of the local UDLD-enabled port.
- Neighbor Information:
  - Device ID—ID of the remote device.
  - Device MAC—MAC address of the remote device.
  - Device Name—Name of the remote device.
  - Port ID—Name of the remote port.
- State—State of the link between the local and neighboring device on the local port. The following values are possible:
  - Detection—The latest UDLD state of the port is in the process of being determined. Expiration time has not yet expired since the last determination (if there was one), or since UDLD began running on the port, so that the state is not yet determined.
  - Bidirectional—Traffic sent by the local device is received by its neighbor, and traffic from the neighbor is received by the local device.
  - Undetermined—The state of the link between the port and its connected port cannot be determined either because no UDLD message was received or the UDLD message did not contain the local device ID in it.
  - Disabled—UDLD has been disabled on this port.
  - Shutdown—The port has been shut down because its link with the connected device is undetermined in aggressive mode.

- Neighbor Expiration Time (Sec.)—Displays the time that must pass before the device attempts to determine the port UDLD status. This is three times the Message Time.
- Neighbor Message Time (Sec.)—Displays the time between UDLD messages.

PoE

A PoE device is Power Sourcing Equipment (PSE) that delivers electrical power to a connected AFAIK PD (powered devices) over existing copper cables without interfering with the network traffic, updating the physical network or modifying the network infrastructure.

PoE provides the following features:

- Eliminates the need to run 110/220 V AC power to all devices on a wired LAN
- Eliminates the need to deploy double cabling systems in an enterprise significantly decreasing installation costs Power over Ethernet can be used in any enterprise network that deploys relatively low-powered devices connected to the Ethernet LAN, such as: IP phones, Wireless access points, IP gateways, Audio, and video remote monitoring devices.

PoE is implemented in the following stages:

- Detection—Sends special pulses on the copper cable. When a PoE device is located at the other end, that device responds to these pulses.
- Classification—Negotiation between the Power Sourcing Equipment (PSE) and the Powered Device (PD) commences after the Detection stage. During negotiation, the PD specifies its class, which indicates the maximum amount of power that the PD consumes.
- Power Consumption—After the classification stage completes, the PSE provides power to the PD. If the PD supports PoE, but without classification, it’s assumed to be class 0 (the maximum). If a PD tries to consume more power than permitted by the standard, the PSE stops supplying power to the port. PoE supports two modes:
  - Port Limit—The maximum power the device agrees to supply is limited to the value the system administrator configures, regardless of the Classification result.
  - Class Power Limit—The maximum power the device agrees to supply is determined by the results of the Classification stage. This means that it’s set as per the Client's request.

Warning The PoE unit shouldn't be connected only to a PoE network and external power at the same time.

Properties

Note This section is only relevant for devices supporting PoE.

The PoE Properties page enables selecting either the Port Limit or Class Limit PoE mode and specifying the PoE traps to be generated. These settings are entered in advance. When the PD actually connects and is consuming power, it might consume much less than the maximum power allowed. Output power is disabled during power-on reboot, initialization, and system configuration to ensure that PDs aren't damaged.

To configure PoE on the device and monitor current power usage:

Procedure

Step 1 Click **Port Management** > **PoE** > **Properties**.

Step 2 Enter the values for the following fields:

- Power Mode—Select one of the following options:
  - Class Limit—Maximum power limit per port is determined by the class of the device, which results from the Classification stage.
  - Port Limit—Maximum power limit per each port is configured by the user.

    Note
    When you change from Port Limit to Class Limit or conversely, disable the PoE ports, and enable them after changing the power configuration.

- Traps—Check **Enable** to enable traps. If traps are enabled, you must also enable SNMP and configure at least one SNMP Notification Recipient.
- Power Trap Threshold—Enter the usage threshold that is a percentage of the power limit. An alarm is initiated if the power exceeds this value.

  The following PoE power information is displayed for the device:
  - Nominal Power—Total amount of power the device can supply to all the connected PDs.
  - Allocated power—The amount of the power that is currently allocated to the PoE ports. The allocated power is calculated by summing the power that is allocated to each of the PoE ports. If the port negotiated power allocation with PD using CDP or LLDP then the port power allocation is based on the results of the CDP or LLDP negotiation. If the port did not negotiate the power using CDP or LLDP then the power allocated to the port equals the PD consumed power.
  - Available Power—Nominal power minus the amount of consumed power.

Note
- Power allocation based on LLDP negotiation may be higher than the negotiated power value.
- Power allocation based on CDP negotiation will be equal to the negotiated power value.
- The power allocated per port (if different from the consumed power value) is indicated in parentheses in the "Power" column (PoE Setting Table).

- Software Version—Displays the software version of the PoE chip.
- PSE Chipset & Hardware Revision—PoE chipset and hardware revision number.

Step 3 Click **Apply** to save the PoE properties.

PoE Settings

The Persistent PoE feature (also referred to as Always On PoE) minimizes the dependency of the PoE operation on the switch's status. Before the introduction of this feature, any disruption in the switch operation such as a reboot or fatal error would also cause a disruption in the PoE operation until the device finished coming back up.

With the persistent PoE, warm reboots such as the ones performed by the reload command or the reboot feature in the GUI will not disrupt the operation of the PoE in it's current state.

The PoE Settings displays the system information for enabling PoE on the interfaces. It monitors the power usage and maximum power limit per port when the PoE mode is Port Limit. When the power consumed on the port exceeds the port limit, the port power is turned off. To configure PoE settings, follow these steps:

Procedure

Step 1 Click **Port Management** > **PoE** > **Settings** .

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

Step 3 Enter the value for the following field:

Note
Ports are displayed with relevant PoE information. These fields are described in the Edit page except for the following fields:

- Administrative Power Allocation (mW)—Enter the amount of power that can be allocated.
- Operational Status—Displays whether PoE is currently active on the port.
- PoE Standard—Displays the type of PoE supported, such as 60W PoE and 802.3 AT PoE.
- Interface—Select the port to configure.
- Administrative Status—Enable or disable PoE on the port.
- Time Range—Select to enable.
- Time Range Name—If Time Range has been enabled, select the time range to be used. Click **Edit** to go to the Time Range page.
- Priority Level—Select the port priority: low, high, or critical, for use when the power supply is low. For example, if the power supply is running at 99% usage and port 1 is prioritized as high, but port 3 is prioritized as low, port 1 receives power and port 3 might be denied power.
- Class—Displays the class of the device, which indicates the maximum power level of the device.
- Max Power Allocation—This field appears only if the Power Mode set in the PoE Properties page is Power Limit. Displays the maximum amount of power permitted on this port.
- Negotiated Power—Power allocated to device.

Note
The "expired" warning may appear alongside the Watt value when power is allocated to the device via CDP or LLDP negotiation. When the switch stops receiving negotiation packets from the powered device, the port enters the expired state. If this happens, the port will supply power based on the most recent negotiation packet received from this device. If the device resends the negotiation packet, the port will exit the expired state and apply power based on the information in the new packet.

- Power Negotiation Protocol—Protocol determining the negotiated power.
- Power Consumption—Displays the amount of power in milliwatts assigned Settings (Class Limit)

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

PoE Settings-Class Limits

The PoE Settings (Class Limit) Settings page displays system PoE information for enabling PoE on the interfaces and monitoring the current power usage and maximum power limit per port.

Note PoE can be configured on the device for a specific period. This feature enables you to define, per port, the days in the week and the hours that PoE is enabled. When the time range is not active, PoE is disabled.

This page limits the power per port based on the class of the connected PD. For these settings to be active, the system must be in PoE Class Limit mode. That mode is configured in the PoE Properties, on page 12. When the power consumed on the port exceeds the class limit, the port power is turned off.

To configure PoE class limit setting, complete the following steps:

Procedure

Step 1 Click **Port Management > PoE > Settings (Class Limit)**.

Ports are displayed with relevant PoE information. These fields are described in the Edit page except for the following fields:

- PoE Standard—Displays the type of PoE supported, such as 60W PoE and 802.3 AT PoE).
- Operational Status—Displays whether PoE is currently active on the port.

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

Step 3 Enter the value for the following field:

- Interface—Select the port to configure.
- Administrative Status—Check to enable.
- Time Range—Select to enabled PoE on the port.
- Time Range Name—If Time Range has been enabled, select the time range to be used. Click **Edit** to go to the Time Range page.

- Priority Level—Select the port priority: low, high, or critical, for use when the power supply is low. For example, if the power supply is running at 99% usage and port 1 is prioritized as high, but port 3 is prioritized as low, port 1 receives power and port 3 might be denied power.
- Auto Class Mode—Check **Enable** to enable auto class mode.
- Initiate Auto Class Process—Check **Enable** to enable initiate auto class mode. (Available only if Auto Class Mode is enabled on the interface).
- Class—Displays the class of the device, which indicates the maximum power level of the device:

Class	Maximum Power Delivered by Device Port
0	15.4 watt or 30.0 watt
1	4.0 watt
2	7.0 watt
3	15.4 watt
4	30.0 watt

- Max Power Allocation—This field appears only if the Power Mode set in the PoE Properties page is Power Limit. Displays the maximum amount of power permitted on this port.

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

PoE Statistics

PoE consumption readings are taken every 1 minute. The daily, weekly, and monthly statistics are saved in flash memory, so that they are still available after reboot. A sample's average PoE consumption per port/device is as follows: Sum of all PoE consumption readings in a period / Number of minutes in the sampling period.

To view the PoE consumption trend on the device and define settings for the view, follow these steps:

Procedure

Step 1 Click **Port Management** > **PoE** > **Statistics**.

Step 2 Select the Interface.

Step 3 Select the Refreshed Rate.

Step 4 The following fields are displayed for the selected interface:

Consumption History

- Average Consumption over Last Hour—Average of all PoE consumption readings in the last hour.
- Average Consumption over Last Day—Average of all PoE consumption readings in the last day.
- Average Consumption over Last Week—Average of all PoE consumption readings in the last week.

PoE Event Counters

- Overload Counter—Number of overload conditions detected.
- Denied Counter—Number of denied conditions detected.
- Absent Counter—Number of absent conditions detected.
- Invalid Signature Counter—Number of invalid signature conditions detected.

Step 5 Click **Clear Event Counters** to clear event counters.

Step 6 Click **View All Interfaces Statistics** to view all interface statistics in a table format.

Step 7 Click **View Interface History Graph**, to view the interface history graph.

Step 8 Click **Refresh** to refresh the data.

Green Ethernet

Green Ethernet is a common name for a set of features that is environmentally friendly, and to reduce the power consumption of a device.

The Green Ethernet feature can reduce overall power usage in the following ways:

- Energy-Detect Mode—On an inactive link, the port moves into inactive mode, saving power while keeping the administrative status of the port Up. Recovery from this mode to full operational mode is fast, transparent, and no frames are lost. This mode is disabled by default.
- Short-Reach Mode—This feature provides for power savings on a short length of cable. After cable length is analyzed, the power usage is adjusted for various cable lengths. If the cable is shorter than 30 meter for 10 gigabit ports and 50 meter for other type of ports, the device uses less power to send frames over the cable, thus saving energy. This mode is only supported on RJ45 ports; it doesn't apply to Combo ports. This mode is disabled by default.

In addition to the preceding Green Ethernet features, the switch supports the 802.3az Energy-Efficient Ethernet (EEE). EEE reduces power consumption when there's no traffic on the port. EEE is enabled globally by default.

Power savings, current power consumption, and cumulative energy saved can be monitored. The total amount of saved energy can be viewed as a percentage of the power that would have been consumed by the physical interfaces had they not been running in Green Ethernet mode. The saved energy displayed is only related to Green Ethernet. The amount of energy saved by EEE isn't displayed.

Properties

The Properties page displays and enables configuration of the Green Ethernet mode for the device. It also displays the current power savings.

To enable Green Ethernet and Energy-Efficient Ethernet (EEE) and view power savings, follow these steps:

Procedure

Step 1 Click **Port Management** > **Green Ethernet** > **Properties**.

Step 2 Configure the values for the following fields:

- Energy Detect Mode—Click the checkbox to enable this mode.
- Short Reach—Click the checkbox to enable this feature.
- Port LEDs—Select to enable the port LEDs. When these are disabled, they don't display link status, activity, etc.
- 802.3 Energy-Efficient Ethernet (EEE)—Globally enable or disable EEE mode. 802.3az EEE is designed to save power when there's no traffic on the link. In Green Ethernet, power is reduced when the port is down. With 802.3az EEE, power is reduced when the port is up, but there's no traffic on it.

  Note
  On Green Ethernet interfaces, the 802.3 EEE is supported for a link speed of 100Mbps and higher. On the 10G interfaces, the 802.3 EEE is supported for a link speed of 1Gbps and higher.

Step 3 Click **Reset Energy Saving Counter**—To reset the Cumulative Energy Saved information.

Step 4 Click **Apply**. The Green Ethernet Properties are written to the Running Configuration file.

Port Settings

The Port Settings displays the current Green Ethernet and EEE modes per port, and enables configuring Green Ethernet on a port using the Edit Port Setting page. For the Green Ethernet modes to operate on a port, the corresponding modes must be activated globally in Properties, on page 17.

EEE works only when ports are set to Auto negotiation. The exception is that EEE is still functional even when Auto Negotiation is disabled, but the port is at 1GB or higher.

To define per port Green Ethernet settings, follow these steps:

Procedure

Step 1 Click **Port Management** > **Green Ethernet** > **Port Settings**.

The Port Settings page displays the following:

- Global Parameter Status-Displays following:
  - Energy Detect Mode-Whether this mode is enabled or not.
  - Short Reach Mode-Whether this mode is enabled.
  - 802.3 Energy Efficient Ethernet (EEE) Mode-Whether this mode is enabled.

  For each port the following fields are described:

Note
Some fields may not be displayed on some SKUs.

- Port—The port number.
- Energy Detect—State of the port regarding the Energy Detect feature:
  - Administrative—Displays whether Energy Detect is enabled.
  - Operational—Displays whether Energy Detect is currently operating on the local port. This is a function of whether it has been enabled (Administrative Status), whether it has been enabled on the local port and whether it is operational on the local port.
  - Reason—Displays the reason that Energy Detect is not operational even if it is enabled.
- Short Reach—State of the port regarding the Short Reach feature:
  - Administrative—Displays whether Short Reach is enabled.
  - Operational—Displays whether Short Reach is currently operating on the local port. This is a function of whether it has been enabled (Administrative Status), whether it has been enabled on the local port and whether it is operational on the local port.
  - Reason—Displays the reason that Short Reach is not operational even if it is enabled.
  - Cable Length—Length of cable.
- 802.3 Energy Efficient Ethernet (EEE)—State of the port regarding the EEE feature:
  - Administrative—Displays whether EEE was enabled.
  - Operational—Displays whether EEE is currently operating on the local port. This is a function of whether it has been enabled (Administrative Status), whether it has been enabled on the local port and whether it is operational on the local port.
  - LLDP Administrative—Displays whether advertising EEE counters through LLDP was enabled.
  - LLDP Operational—Displays whether advertising EEE counters through LLDP is currently operating.
  - EEE Support on Remote—Displays whether EEE is supported on the link partner. EEE must be supported on both the local and remote link partners.

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

Step 3 Select the Interface and configure the options available for the port by checking **Enable** for each option.

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