

Port Management

This chapter contains the following sections:

- Port Settings, on page 1
- Error Recovery Settings, on page 4
- Loopback Detection Settings, on page 5
- Link Aggregation, on page 5
- Power over Ethernet, on page 9
- Green Ethernet, on page 12

Port Settings

The Port Settings page displays the global and per port setting of all the ports. Here, you can select and configure the desired 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 Enter the following fields:

- Jumbo Frames—Check to support packets of up to 10 KB in size. If Jumbo Frames isn't enabled (default), the system supports packet size up to 1522 bytes.

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 desired port, and click **Edit.**

Step 5 Modify the following parameters:

Interface	Select the port number.

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.
Administrative Status	Select whether the port must be Up or Down when the device is rebooted.
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
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 is effective only when the port is administratively Up.
Time Range Name	Select the profile that specifies the time range.
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, and Flow Control abilities 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 the port duplex mode. This field is configurable only when auto-negotiation is disabled, and the port speed is set to 10M or 100M. At port speed of 1G or 10G, the mode is always full-duplex. The possible options are: • Half—The interface supports transmission between the device and the client in only one direction at a time. • Full—The interface supports transmission between the device and the client in both directions simultaneously.
Operational Duplex Mode	Displays the ports current duplex mode.

Auto Advertisement Speed	Select the capabilities advertised by auto-negotiation when it is enabled. **Note** Not all options are relevant for all devices. The options are: • All Speed—All port speeds and duplex mode settings can be accepted. • 10M—10 Mbps speed • 100M—100 Mbps speed • 1000M—1000 Mbps speed • 10M/100M—10 and 100 Mbps speeds • 10G—10 Gbps speed
Operational Advertisement	Displays the capabilities currently published to the ports neighbor. The possible options are those specified in the Administrative Advertisement field.
Auto Advertisement Duplex	Select the duplex mode to be advertised by the port. The options are: • All Duplex—All duplex modes can be accepted. • Full—The interface supports transmission between the switch and the client in both directions simultaneously. • Half—The interface supports transmission between the switch and the client in only one direction at a time
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, or enable the auto-negotiation of Flow Control on the port (only when in Full Duplex mode). Flow control auto-negotiation can’t be enabled on combo ports.
Protected Port	Check Enable to make this a 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 Link Aggregation Groups (LAGs)) that share the same Broadcast domain (VLAN). • Packets received from protected ports can 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 is not subject to VLAN membership. Devices connected to protected ports are not 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.Both ports and LAGs can be defined as protected or unprotected.

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
  - 802.1x Single Host Violation—Select to enable automatic error recovery when the port is shut down by 802.1x.
  - ACL —Select to enable automatic error recovery mechanism by an ACL action.
  - BPDU—Enable automatic recovery when the port is shut down by STP Loopback Guard.
  - Broadcast Flood—Select to enable automatic error recovery from the Broadcast flood
  - DHCP Rate Limit—Check Enable to enable the timer to recover from the DHCP rate limit causes.
  - ARP Inspection—Check Enable to the timer to recover from the ARP inspection causes
  - PoE— Select Enable to enable the timer to recover from the Power over Ethernet (PoE) causes
  - Loopback Detection—Select to enable error recovery mechanism for ports shut down by loopback detection.
  - Port Security—Select to enable automatic error recovery when the port is shut down for port security violations.
  - Self Loop—Select Enable to enable the timer to recover from the self loop cause
  - Unicast Flood— Select Enable to enable the timer to recover from the Unicast flood causes.
  - Unknown Multicast Flood— Select Enable to enable the timer to recover from the unknown Multicast flood causes.

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

To manually reactivate a port:

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

The list of inactivated interfaces along with their Suspension Reason is displayed.

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.

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.

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.
Time Range	Select to enable the 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.
Time Range Name	Select the profile that specifies the time range. If a time range is not yet defined, click **Edit** to go to 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.
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 and flow control to its partner (the Flow Control default is disabled). 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 Port Speed	Select the speed of the ports in the LAG.
Back Pressure	Check the **Enable** check box in the Back Pressure area to slow down packet reception speed when the device is congested. This feature is used with half duplex mode, and disables the remote port by preventing it from sending packets and jamming the signal.
Auto Advertisement Speed	Select the capabilities to be advertised by the LAG. The options are: • All Speed—All LAG speeds and both duplex modes are available.

Option	Description
	• 10M—The LAG advertises a 10 Mbps speed and the mode is full duplex. • 100M—The LAG advertises a 100 Mbps speed and the mode is full duplex. • 1000M—The LAG advertises a 1000 Mbps speed and the mode is full duplex. • 10/100M—The LAG advertises a 10/100 Mbps speed and the mode is full duplex. • 10G—The LAG advertises a 10G speed and the mode is full duplex.
Flow Control	Set Flow Control to either Enable or Disable or enable the Auto-Negotiation of Flow Control 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.
Current Flow Control	Displays the current Flow Control setting.

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

Link Aggregation Control Protocol (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.

Power over Ethernet

This section describes how to use the PoE feature.

A PoE device is Power Sourcing Equipment (PSE) that delivers electrical power to a connected Pod Devices (PD) 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-pod devices connected to the Ethernet LAN, such as: IP phones, Wireless access points, IP gateways, Audio and video remote monitoring devices.

PoE implements 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 Pod Device (PD) commences after the Detection stage. During negotiation, the PD specifies its class, which indicates 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 is 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 is set as per the Client's request.

Warning The PoE unit is to be connected only to PoE networks without routing to the outside plant.

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—Enable or disable 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 counters are displayed for the device:
  - Operational Status—Displays the operational status (Normal or Fault) of the PoE switch.
  - Nominal Power—Total amount of power the device can supply to all the connected PDs.
  - Consumed Power—Amount of power currently being consumed by the PoE ports.
  - Available Power—Nominal power minus the amount of consumed power.
- 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 Port Settings

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** > **PoE Port Settings** .

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

Step 3 Enter the value for the following field:

- Interface—Select the port to configure.
- PoE 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. Time ranges are defined in Time Range. Click **Edit** to go to the Time Range page.
- Power 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.
- Administrative Power Allocation—If the Power mode is Port Limit, enter the power in milliwatts allocated to the port (Range: 0 - 30000. Default: 30000).
- 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.
- Power Consumption—Displays the amount of power in milliwatts assigned to the powered device connected to the selected port.
- 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
1	4.0 watt
2	7.0 watt
3	15.4 watt
4	30.0 watt

- Overload Counter—Displays the number of overload counters

- Short Counter—Displays the number of short counters
- Denied Counter—Displays the number of denied counters
- Absent Counter—Displays the number of absent counters
- Invalid Signature Counter—Displays the times that an invalid signature was received. Signatures are the means by which the powered device identifies itself to the PSE. Signatures are generated during powered device detection, classification, or maintenance.

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

Green Ethernet

Green Ethernet is a common name for a set of features that is designed to be environmentally friendly, and to reduce the power consumption of a device. Green Ethernet is different from EEE in that Green Ethernet energy-detect is enabled on all devices whereas only Gigabyte ports are enable with EEE.

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.

In addition to the above Green Ethernet features, the 802.3az Energy Efficient Ethernet (EEE) is found on devices supporting GE ports. EEE reduces power consumption when there is 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 is not displayed.

Green Ethernet 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 EEE and view power savings, follow these steps:

Procedure

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

Step 2 Enter the values for the following fields:

- 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 is 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 is no traffic on it.

Step 3 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 Green Ethernet Properties, on page 12.

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:

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

Step 3 Select to enable or disable 802.3 Energy Efficient Ethernet (EEE) mode on the port.

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