ECS1100 Series

Release v1.0.1.2

Web Management Guide

www.edge-core.com

Web Management Guide

ECS1100-5P

L2 Gigabit Ethernet Web Managed PoE Switch
with 4 1000BASE-T RJ-45 PoE+ (30W) Ports,
and 1 1000BASE-T RJ-45 Port

ECS1100-10HP

L2 Gigabit Ethernet Web Managed PoE Switch
with 4 1000BASE-T RJ-45 PoE++ (90W) Ports,
4 1000BASE-T RJ-45 PoE+ (30W) Ports,
and 2 100/1000M SFP Ports

ECS1100-28HP

L2 Gigabit Ethernet Web Managed PoE Switch
with 8 1000BASE-T RJ-45 PoE++ (90W) Ports,
16 1000BASE-T RJ-45 PoE+ (30W) Ports,
and 4 100/1000M SFP Ports

E122023-CS-R02

How to Use This Guide

This guide includes detailed information on the switch software, including how to operate and use the management functions of the switch. To deploy this switch effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all of its software features.

Who Should Read This Guide?

This guide is for network administrators who are responsible for operating and maintaining network equipment. The guide assumes a basic working knowledge of LANs (Local Area Networks), the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

How This Guide is Organized

This guide describes the switch's web browser interface.

The guide includes these sections:

- Section I "Getting Started" — Includes basic settings required to access the management interface.
- Section II "Web Configuration" — Includes all management options available through the web browser interface.
- Section III "Appendices" — Includes information on troubleshooting device management access.

Related Documentation

This guide focuses on software configuration through a web browser.

For information on how to install the switch and all safety information and regulatory statements, see the following documents:

Quick Start Guide
Safety and Regulatory Information

Conventions

The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warning: Alerts you to a potential hazard that could cause personal injury.

Revision History

This section summarizes the changes in each revision of this guide.

December 2023 Revision

This is the second version of this guide. This guide is valid for software release v1.0.1.2 and includes these changes:

- Added support for ECS1100-28HP
- Updated "Port Trunk" on page 26 for ECS1100-28HP
- Updated "PoE Port Config" on page 40 for ECS1100-28HP
- Updated "PoE Extend Mode" on page 46

August 2023 Revision

This is the first version of this guide. This guide is valid for software release v1.0.1.0.

Contents

Section I

Getting Started

This section describes the basic settings required to access the management interface.

This section includes these chapters:

1 Using the Web Interface

This switch provides an embedded HTTP web management interface. Using a web browser you can configure the switch and view statistics to monitor network activity. The web management interface can be accessed by any computer on the network using a standard web browser.

Connecting to the Web Interface

Prior to accessing the switch from a web browser, be sure you have first performed the following tasks:

1. The default IP address and subnet mask for the switch is 192.168.2.10 and 255.255.255.0, with no default gateway. If this is not compatible with the subnet connected to the switch, you can configure it with a valid IP address, subnet mask, and default gateway.

2. Set user names and passwords. Access to the web interface is controlled by a default user name and password. For security reasons, you should change the default password and configure new user accounts as soon as possible. (See "Account Settings" on page 17.)

3. After you enter a user name and password, you will have access to the web management interface.

Note: Users are automatically logged off of the web server if no input is detected for 6 minutes.

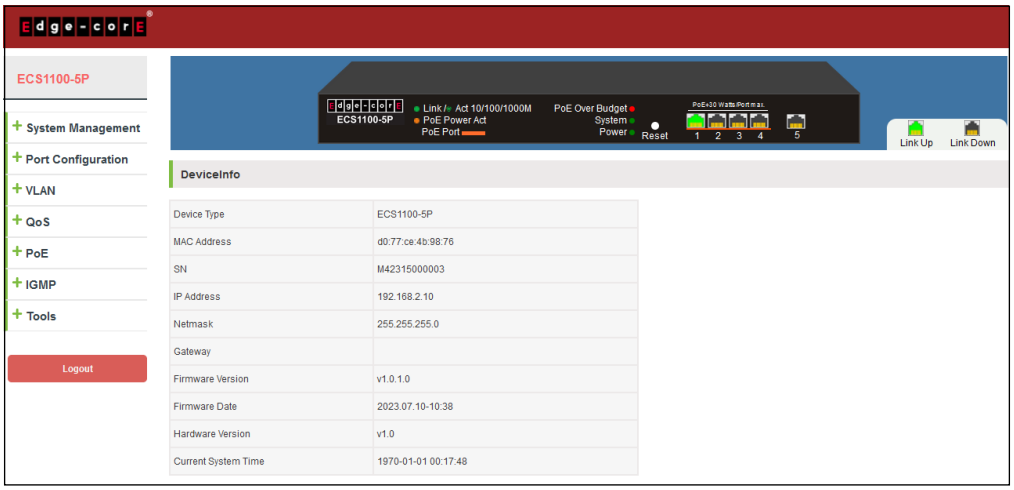
Navigating the Web Browser Interface

To access the web-browser interface you must first enter a user name and password. The administrator has read/write access to all configuration parameters and statistics. The default user name and password for the administrator is "admin." The administrator has full access privileges to configure any parameters in the web interface. Refer to "Account Settings" on page 17 for more details.

Dashboard

When your web browser connects with the switch's web agent, the Dashboard is displayed as shown below. The Dashboard displays the main menu on the left side of the screen and System Information on the right side. The main menu links are used to navigate to other menus, and display configuration parameters and statistics.

Figure 1: Dashboard



Configuration Options

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the Apply button to confirm the new setting.

The following table summarizes some common web page configuration buttons.

Table 1: Web Page Configuration Buttons

Button	Action
Apply	Sets specified values to the system.
Select All	Selects all entries in a table.
Delete	Deletes the selected items.

Table 1: Web Page Configuration Buttons (Continued)

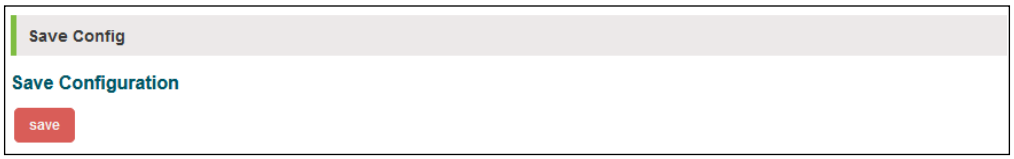
Button	Action
Refresh	Refreshes screen information.
Clear	Clears all current information.
Add / Modify	Adds or modifies a table entry.
Logout	Ends the current web management session.

Saving the Configuration

The switch configuration settings are not automatically saved by the system for subsequent use when the switch is rebooted. You must save these settings to a configuration file on the switch.

The Apply button only saves settings for the current session. To save all configuration settings for each reboot, use the Save button on the Tools > Backup Restore page.

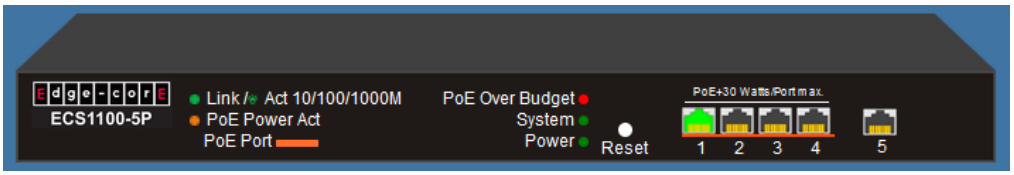
Figure 2: Saving the Switch Configuration



Panel Display

The web agent displays an image of the switch's ports.

Figure 3: Front Panel Indicators



Note: This manual covers the ECS1100-5P, ECS1100-10HP, and ECS1100-28HP switches. Other than the difference in the number and types of ports there are no significant differences. Therefore, the screen display examples in this manual might be based on any of the switch models in this series.

Main Menu

Using the web interface, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions.

The main menu is organized as follows:

- **System Management** — System Information, IP Settings, Account Settings, System Time, Cloud Manage, Jumbo Frames
- **Port Configuration** — Port Settings, Storm Control, Port Speed Limit, Port Trunk, Port Statistics, SFP
- **VLAN** — Static VLAN, VLAN Setting
- **QoS** — QoS Basic, QoS Advanced
- **PoE** — PoE Port Config, PoE System Power, PD Alive, PoE Timer Rule, PoE Timer Set, PoE Extend Mode
- **IGMP** — IGMP Snooping, Router Port, Group Address
- **Tools** — System Upgrade, Backup Restore, System Reset, System Reboot

Section II

Web Configuration

This section describes switch configuration features, along with a description of how to configure each feature via a web browser.

This section includes these chapters:

2 System Management

The system management pages are used to control IP settings, user names and passwords, system time, and display or configure a variety of other system information.

This chapter describes the following topics:

- System Information — Displays basic switch information, including hardware and software versions.
- IP Settings — Sets an IPv4 address for management access.
- Account Settings — Manually configure access rights on the switch for specified users.
- System Time — Sets the current time manually or through specified NTP or SNTP servers.
- Cloud Manage — Enables ecCLOUD management.
- Jumbo Frames — Enables support for jumbo frames.

System Information

Use the System Management > System Information page to display hardware/ firmware version numbers for the main board and management software, as well as the power status of the system.

Parameters

The following parameters are displayed:

- **Device Type** — The model number of the switch.
- **MAC Address** — The MAC address assigned to the switch.
- **SN** — The serial number of the switch.
- **IP Address** — The IPv4 address assigned to the switch. (Default: 192.168.2.10)
- **Netmask** — The network mask that identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)

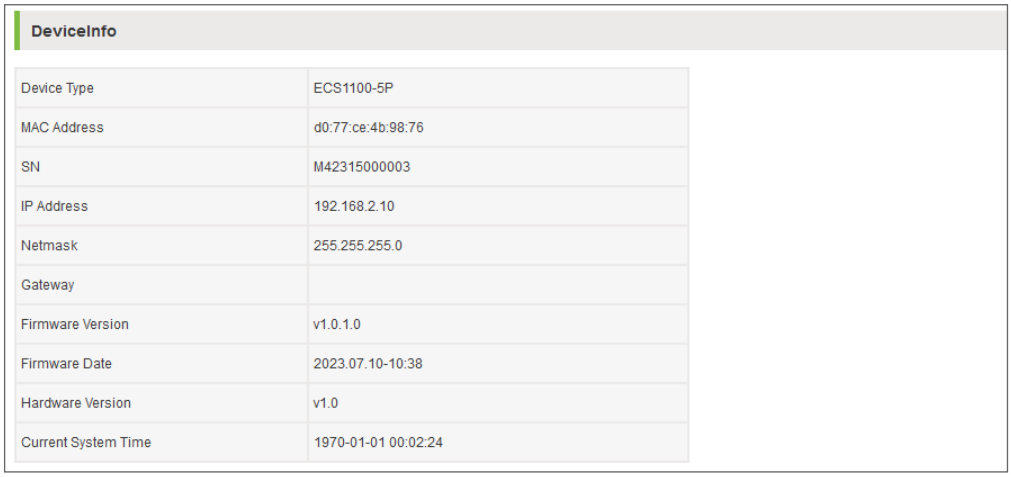
- **Gateway** — The default gateway address for destinations not found in local routing tables. (Default: None)
- **Firmware Version** — The version number of the runtime code.
- **Firmware Date** — The date of the runtime code.
- **Hardware Version** — The hardware version of the switch.
- **Current System Time** — Shows the current time set on the switch.

Web Interface

To view hardware and software version information.

1. Click System Management, then System Information.

Figure 4: System Information



IP Settings

Use the System Management > IP Settings page to configure an IPv4 address for the switch. The IPv4 address is set to 192.168.2.10 by default. You might need to change the switch's default settings to values that are compatible with your network, and also set a default gateway between the switch and management stations that exist on another network segment.

You can configure the switch to obtain an address from a DHCP server, or manually configure a static IP address. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything other than this format will not be accepted.

Parameters

The following parameters are displayed:

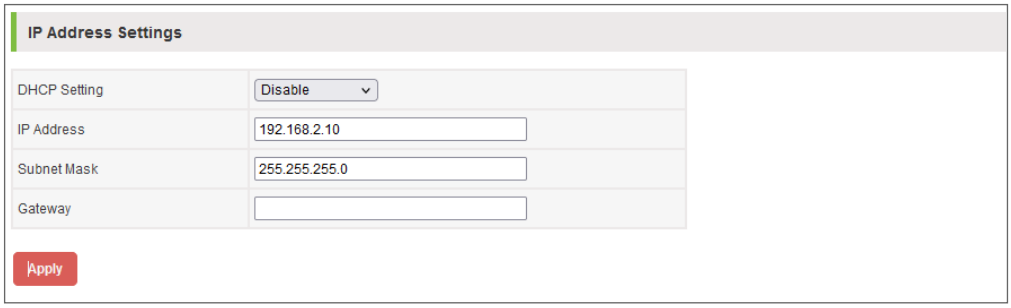
- **DHCP Setting** — Specifies whether IP functionality is enabled via the Dynamic Host Configuration Protocol (DHCP). If DHCP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. DHCP responses can include the IP address, subnet mask, and default gateway. (Default: Disabled)
- **IP Address** — The IPv4 address assigned to the switch. (Default: 192.168.2.10)
- **Subnet Mask** — The network mask that identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)
- **Gateway** — The default gateway address for destinations not found in local routing tables. (Default: None)

Web Interface

To configure a static IP address:

1. Click System Management, then IP Settings.
2. Leave the DHCP Setting as disabled.
3. Enter an IPv4 address and subnet mask for the switch.
4. Optionally enter an IPv4 address for the default gateway.
5. Click Apply

Figure 5: Setting an IP Address



Note: If you change the IP address you will lose access to the web interface. Restart a web interface session using the new configured IP address.

Account Settings

Use the System Management > Account Settings page to control management access to the switch based on a manually configured user name and password.

Usage Guidelines

- The default administrator name is "admin" with the password "admin."
- The administrator has write access for all parameters governing the switch. You should therefore assign a new administrator password as soon as possible, and store it in a safe place.

Parameters

These parameters are displayed:

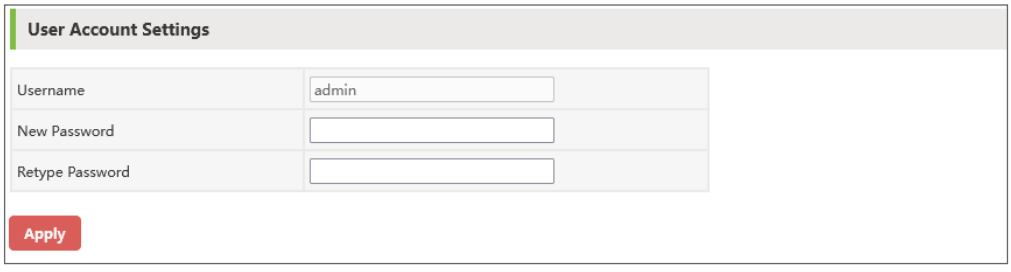
- **Username** — The name of the user. The default is "admin" and this cannot be changed.
- **New Password** — Specifies the user password. (Range: 0-32 characters, case sensitive)
- **Retype Password** — Re-type the password entered in the previous field to ensure no errors were made. The switch will not change the password if these two fields do not match.

Web Interface

To configure a user name and password:

1. Click System Management, then Account Settings.
2. Enter a new password for the switch.
3. Retype the new password for verification.
4. Click Apply

Figure 6: Account Settings



System Time

The Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server. Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock. If the clock is not set manually or via SNTP, the switch will only record the time from the factory default set at the last bootup.

When the SNTP client is enabled, the switch periodically sends a request for a time update to a configured time server. You can configure up to two time server IP addresses. The switch will attempt to poll each server in the configured sequence.

Setting the Time Manually

Use the System Management > System Time page to set the system time on the switch manually without using SNTP.

Parameters

The following parameters are displayed:

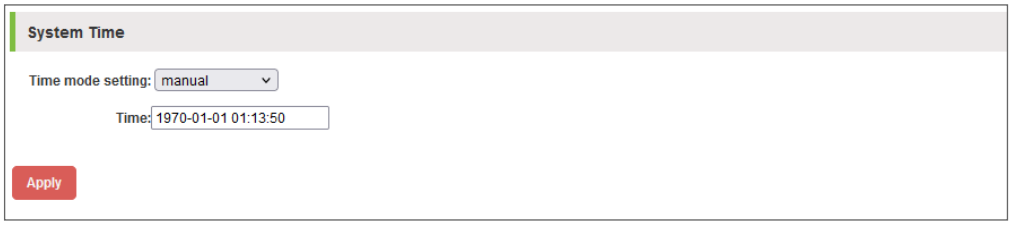
- **Time Mode Setting** — Selects "manual" or "sntp" for setting the time. (Default: manual)
- **Time** – Sets the time on the switch. Enter the date and time in the following format "YYYY-MM-DD hh:mm:ss". (Year Range: 1970-2037; Month Range: 1-12; Day Range: 1-31; Hour Range: 0-23; Minutes Range: 0-59; Seconds Range: 0-59)

Web Interface

To manually set the system time:

1. Click System Management, then System Time.
2. Select "manual" as the mode.
3. Enter the date and time in the Time field.
4. Click Apply

Figure 7: Manually Setting the System Time



Setting the Time Using SNTP

Use the System Management > System Time page to set the system time on the switch using SNTP.

Parameters

The following parameters are displayed:

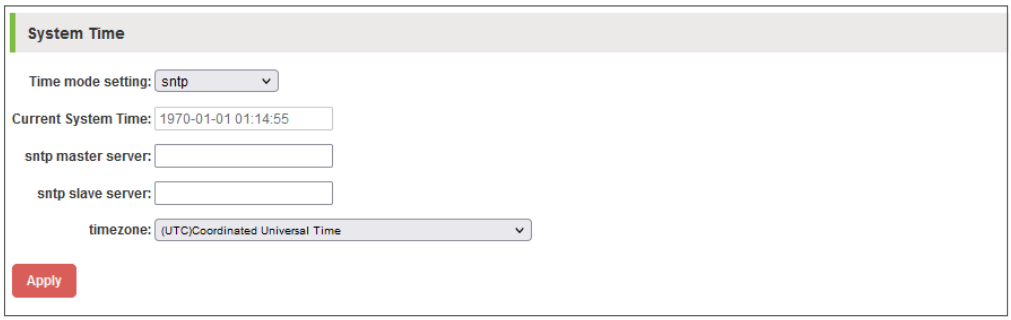
- **Time Mode Setting** — Selects "manual" or "sntp" for setting the time. (Default: manual)
- **Current System Time** — Shows the current time set on the switch.
- **SNTP Master Server** — Sets the IPv4 address for the primary time server.
- **SNTP Slave Server** — Sets the IPv4 address for the secondary time server. The switch attempts to update the time from the primary server, if this fails it attempts an update from the secondary server.
- **Timezone** — To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC (Coordinated Universal Time or UTC, formerly Greenwich Mean Time). A drop-down box provides access to predefined time zone configurations. Each choice indicates it's offset from UTC and lists at least one major city or location covered by the time zone.

Web Interface

To set the time using SNTP:

1. Click System Management, then System Time.
2. Select "sntp" as the mode.
3. Enter IPv4 addresses for the master and slave SNTP servers.
4. Select your local time zone from the list.
5. Click Apply

Figure 8: Using SNTP to Set the System Time



Cloud Manage

Use the System Management > Cloud Manage page to configure the cloud management agent on the switch for management through ecCLOUD.

Edgecore ecCLOUD is a cloud-based network service available from anywhere through a web-browser interface. The switch can be managed by ecCLOUD once you have set up an account and registered the device on the system.

By default, the cloud management agent is disabled on the switch. Setting the cloud management agent to enabled allows the switch to be managed through the ecCLOUD system after the next reboot.

Parameters

The following parameters are displayed:

- **Enable Agent** — Click the checkbox to enable the switch to be managed through the ecCLOUD system.
- **DNS** — Enter the IPv4 address of a Domain Name Server.
- **Registration URL** — Displays the configured cloud registration URL.

Web Interface

To enable cloud management:

1. Click System Management, then Cloud Manage.
2. Click the Enable Agent checkbox.
3. Enter a DNS server IPv4 address.
4. Click Apply
5. Reboot the switch.

Figure 9: Enabling Cloud Management

Jumbo Frames

Use the System Management > Jumbo Frames page to configure support for layer 2 jumbo frames. The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 15K bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

Usage Guidelines

To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

Parameters

The following parameters are displayed:

- **Jumbo Frame Setting** — Configures support for jumbo frames up to 15 KB. (Default: Disabled)

Web Interface

To configure support for jumbo frames:

1. Click System Management, then Jumbo Frames.
2. Enable or disable support for jumbo frames.
3. Click Apply.

Figure 10: Jumbo Frames

3 Port Configuration

The port configuration pages are used to display or set communication parameters for Ethernet ports, configure trunks, and set storm control or port speed limits.

This chapter describes the following topics:

- Port Settings — Configures connection settings, including auto-negotiation, or the manual setting of speed, duplex mode, and flow control.
- Storm Control — Sets the traffic storm threshold for each port.
- Port Speed Limit — Sets input and output rate limits for each port.
- Port Trunk — Configures static trunks.
- Port Statistics — Shows port statistics in table form.
- SFP — Displays SFP transceiver information.

Port Settings

Use the Port Configuration > Port Settings page to enable/disable an interface, set auto-negotiation, or manually fix the speed, duplex mode, and flow control.

Usage Guidelines

The Rate/Duplex mode is fixed at 1000M/Full for Gigabit transceivers and 100M/Full for 100 Mbps transceivers.

Parameters

These parameters are displayed:

- **Port** — The port number.
- **State** — Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable an interface for security reasons. (Default: Enabled)
- **Rate/Duplex** — Allows auto-negotiation to be enabled/disabled. When auto-negotiation is disabled, you can force the settings for speed and mode.

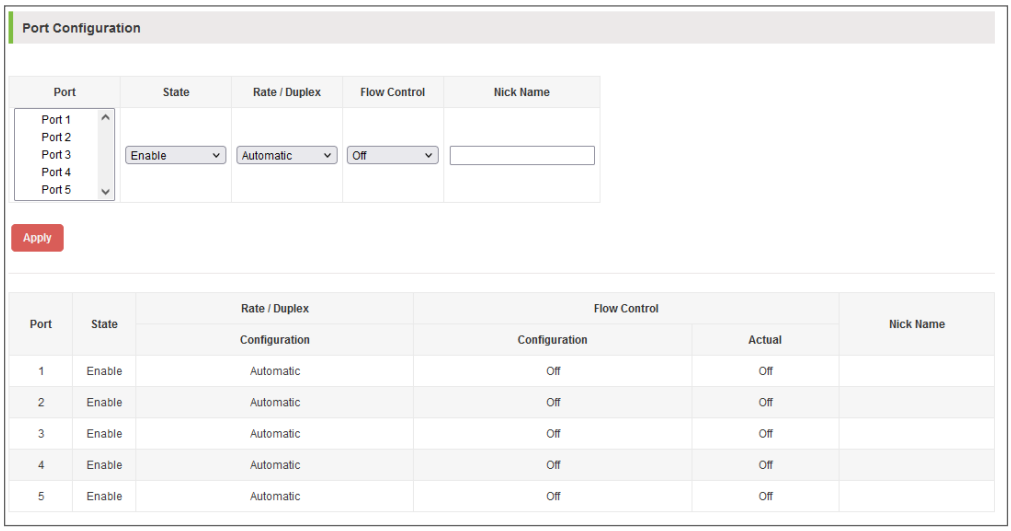
- **Flow Control** — Enables flow control on the port. Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. (Default: Disabled)
- **Nick Name** — Allows you to label an interface. (Range: 1-64 characters)

Web Interface

To configure port settings:

1. Click Port Configuration, then Port Settings.
2. Select one or more port numbers.
3. Set the State to enable.
4. Optionally configure the Rate/Duplex and Flow Control.
5. Click Apply.

Figure 11: Configuring Port Settings



Storm Control

Use the Port Configuration > Storm Control page to configure broadcast, multicast, and unknown unicast storm control thresholds. Traffic storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from traffic storms by setting a threshold for broadcast, multicast or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped.

Usage Guidelines

- Storm Control for broadcast, unknown multicast, and unknown unicast traffic is disabled by default.
- When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.
- Using both rate limiting (Port Speed Limit) and storm control on the same interface may lead to unexpected results. It is therefore not advisable to use both of these features on the same interface.

Parameters

These parameters are displayed:

- **Port** — Displays a list of ports to select. Trunk ports cannot be selected.
- **Broadcast** — Specifies storm control for broadcast traffic.
- **Unknown Unicast** — Specifies storm control for unknown unicast traffic.
- **Unknown Multicast** — Specifies storm control for unknown multicast traffic.
- **State** — Enables or disables storm control. (Default: Disabled for broadcast, unknown multicast, and unknown unicast)
- **Speed** — Threshold level in 1000 bits per second. (Range: 1-1000000 kbps; Default: 0, disabled)

Web Interface

To configure port storm control:

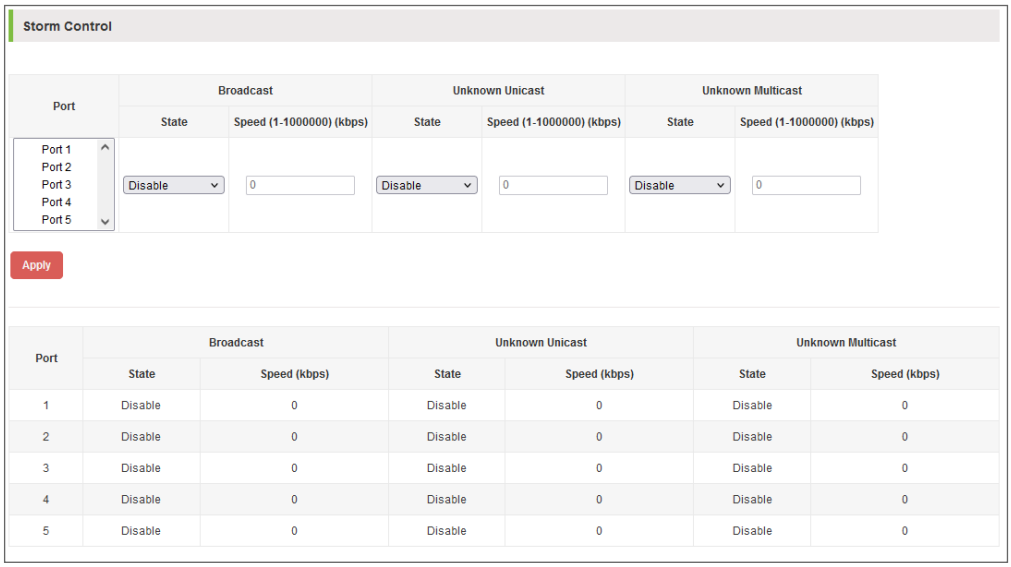
1. Click Port Configuration, then Storm Control.
2. Select one or more ports to configure.

3. Set the State for broadcast, unknown multicast, or unknown unicast to enable.

4. Set the threshold level speed for each traffic type.

5. Click Apply.

Figure 12: Configuring Storm Control



Port Speed Limit

Use the Port Configuration > Port Speed Limit page to apply rate limiting to ingress or egress ports. This function allows the network manager to control the maximum rate for traffic received or transmitted on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Parameters

These parameters are displayed:

- **Port** — Displays a list of switch ports.
- **Ingress** — The port rate limit for received traffic.
- **Egress** — The port rate limit for transmitted traffic.
- **State** — Enables or disables the rate limit. (Default: Disabled)

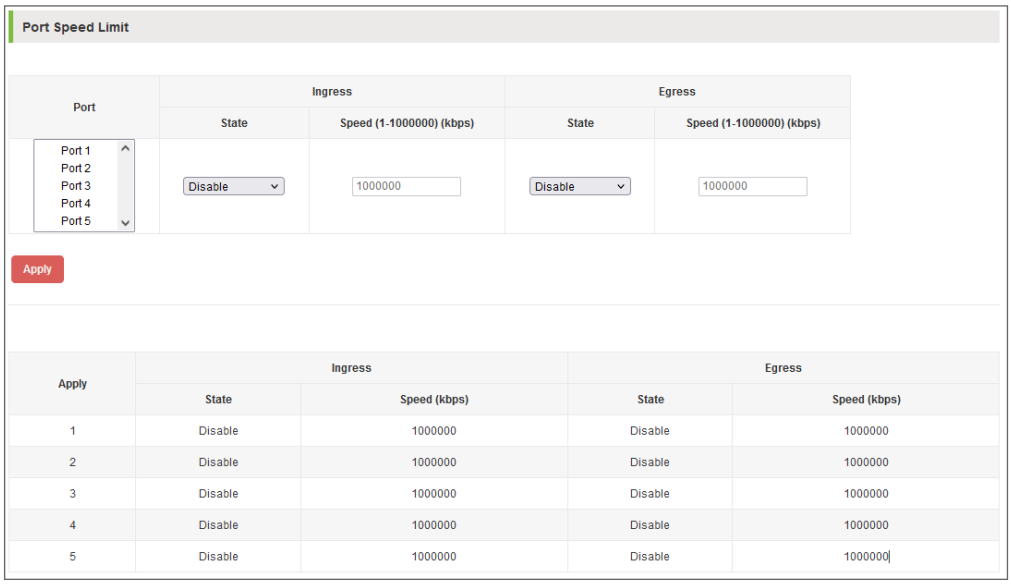
- **Speed** — Sets the rate limit level in 1000 bits per second. (Range: 1-1000000 kbps; Default: 1000000)

Web Interface

To configure port speed limits:

1. Click Port Configuration, then Port Speed Limit.
2. Select one or more port numbers.
3. Set the State for ingress and/or egress to enable.
4. Set the speed limit level for ingress and/or egress traffic.
5. Click Apply.

Figure 13: Configuring Port Speed Limits



Port Trunk

Use the Port Configuration > Port Trunk page to create assign member ports to a trunk.

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers an increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices.

Usage Guidelines

- To avoid creating a loop, configure the trunks before you connect the corresponding network cables between switches.

- You can create up to 2 trunks on the ECS1100-5P and ECS1100-10HP switches, and up to 4 trunks on the ECS1100-28HP switch.
- The ports at both ends of a connection must be configured as trunk ports.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and QoS settings.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- VLAN and IGMP settings can only be made for the entire trunk.

Parameters

These parameters are displayed:

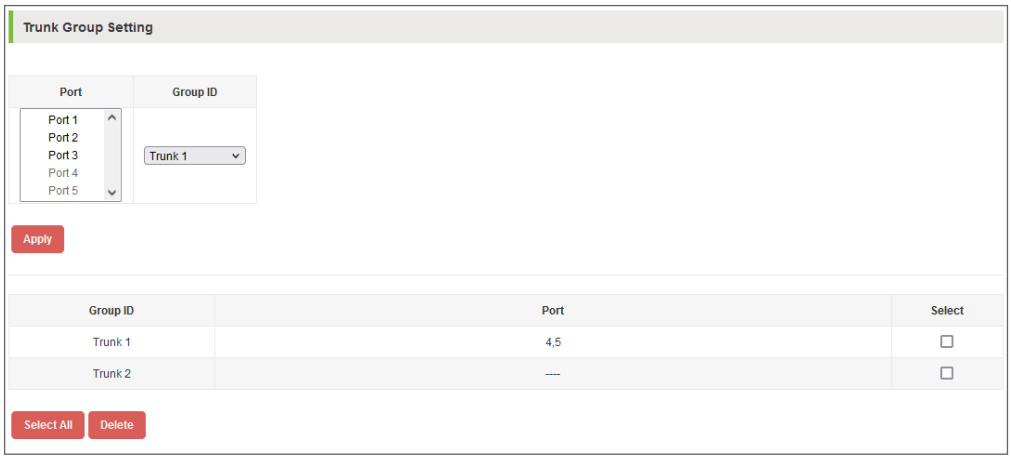
- **Port** — Selects one or more ports to add as trunk members.
- **Group ID** — Trunk identifier. (Range: 1-2 for ECS1100-5P and ECS1100-10HP, and 1-4 for ECS1100-28HP)

Web Interface

To configure port trunk settings:

1. Click Port Configuration, then Port Trunk.
2. Select one or more port numbers to add to a trunk.
3. Select the trunk number (Group ID).
4. Click Apply.

Figure 14: Configuring Port Trunks



Port Statistics

Use the Port Configuration > Port Statistics page to display standard statistics on network traffic. Port statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch or network (such as a faulty port or unusually heavy loading).

Parameters

These parameters are displayed:

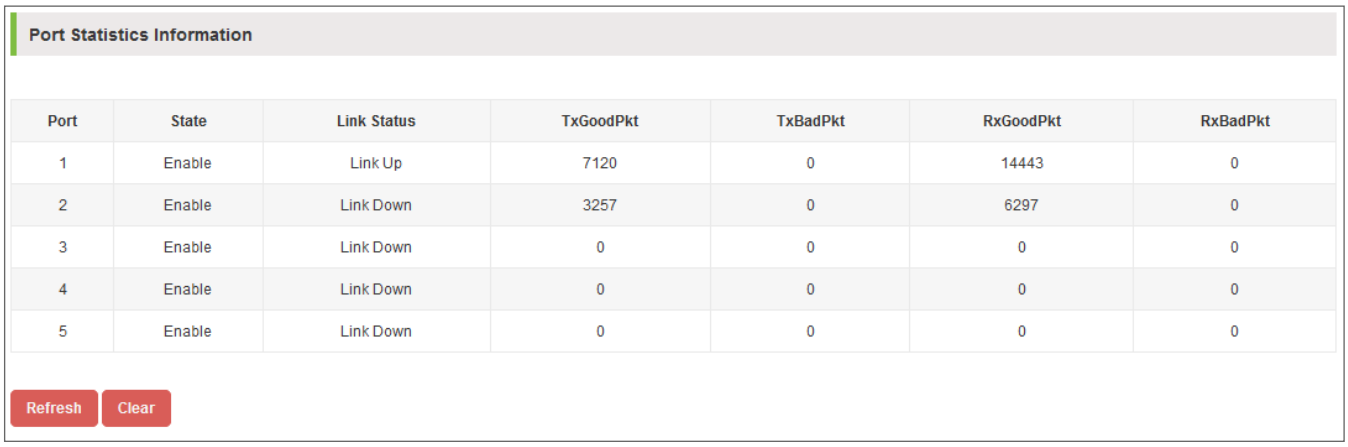
- **Port** — The port number.
- **State** — The administrative state of the port (enabled or disabled).
- **Link Status** — Indicates if the port has a valid link (up or down).
- **TxGoodPkt** — The number of good packets transmitted from the port.
- **TxBadPkt** — The number of outbound packets that could not be transmitted because of errors.
- **RxGoodPkt** — The number of good packets received on the port.
- **RxBadPkt** — The number of received packets that contained errors.

Web Interface

To display port statistics:

1. Click Port Configuration, then Port Statistics.
2. Use the Refresh button to update the page or the Clear button to reset all counters to zero.

Figure 15: Displaying Port Statistics



SFP

Use the Port Configuration > SFP page to display SFP transceiver information. This page applies only to the ECS1100-10HP and ECS1100-28HP switches.

Parameters

These parameters are displayed:

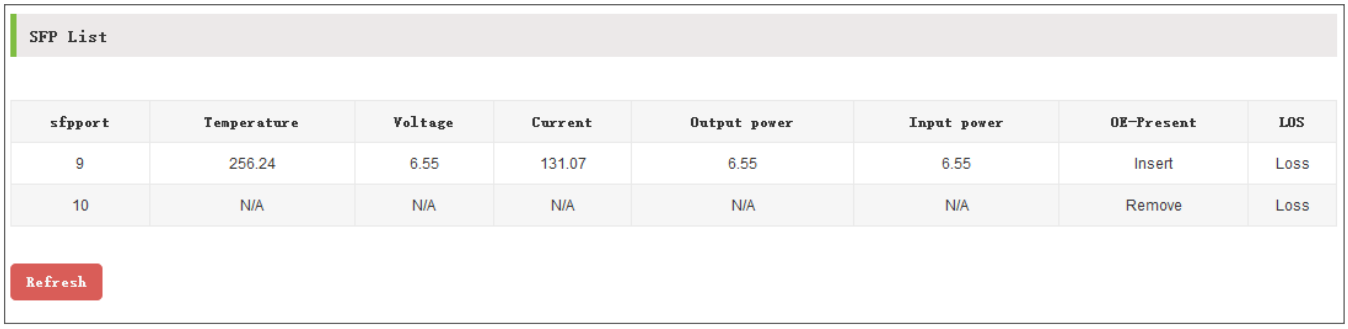
- **sfpport** — The SFP port number.
- **Temperature** — The transceiver working temperature.
- **Voltage** — The transceiver working voltage.
- **Current** — The transceiver working current.
- **Output power** — The transceiver transmit power.
- **Input power** — The transceiver receive power.
- **OE-Present** — Indicates if an optical transceiver is inserted in the slot.
- **LOS** — Indicates a receive loss of signal on the link or no cable connected.

Web Interface

To display SFP port information:

1. Click Port Configuration, then SFP.
2. Use the Refresh button to update the page information.

Figure 16: Displaying SFP Port Information



4 VLAN Configuration

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. The VLAN pages in the web interface describe how to create VLAN groups, add port members, and specify how VLAN tagging is used.

This chapter describes the following topics:

- Static VLAN — Create VLANs and add port members.
- VLAN Setting — Configures a management VLAN and port VLAN IDs.

Static VLAN

Use the VLAN > Static VLAN page to create or remove VLAN groups and add port members.

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Assign ports to VLANs as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices.

Usage Guidelines

- If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you should create a VLAN for that group and enable tagging on all ports.
- Ports can be assigned to multiple tagged or untagged VLANs.
- VLAN 1 is the default untagged VLAN containing all ports on the switch.

Parameters

These parameters are displayed:

- **VLAN ID** — ID of a VLAN (1-4094).
- **VLAN Name** — A name for the VLAN (1 to 32 characters).
- **Port** — Lists the switch port numbers.

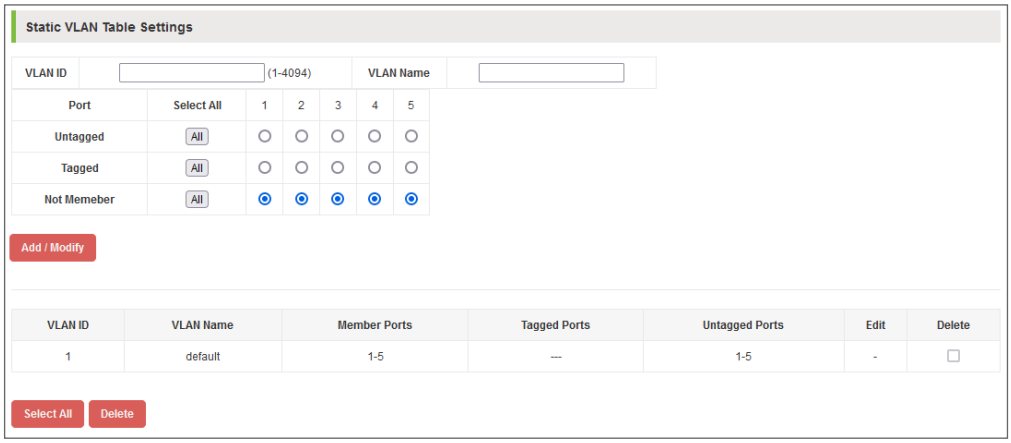
- **Untagged** — A port is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a VLAN tag.
- **Tagged** — A port is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a VLAN tag.
- **Not Member** — A port is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the port.

Web Interface

To configure a static VLAN:

1. Click VLAN, then Static VLAN.
2. Configure a VLAN ID and optionally a VLAN name.
3. Select one or more port numbers as tagged or untagged members.
4. Click Add/Modify.

Figure 17: Configuring Static VLANs



VLAN Setting

Use the VLAN > VLAN Setting page to configure a management VLAN and set the default VLAN identifier (PVID) for ports.

Usage Guidelines

You can access the web interface only when the port PVID is the same as the management VLAN ID.

Parameters

These parameters are displayed:

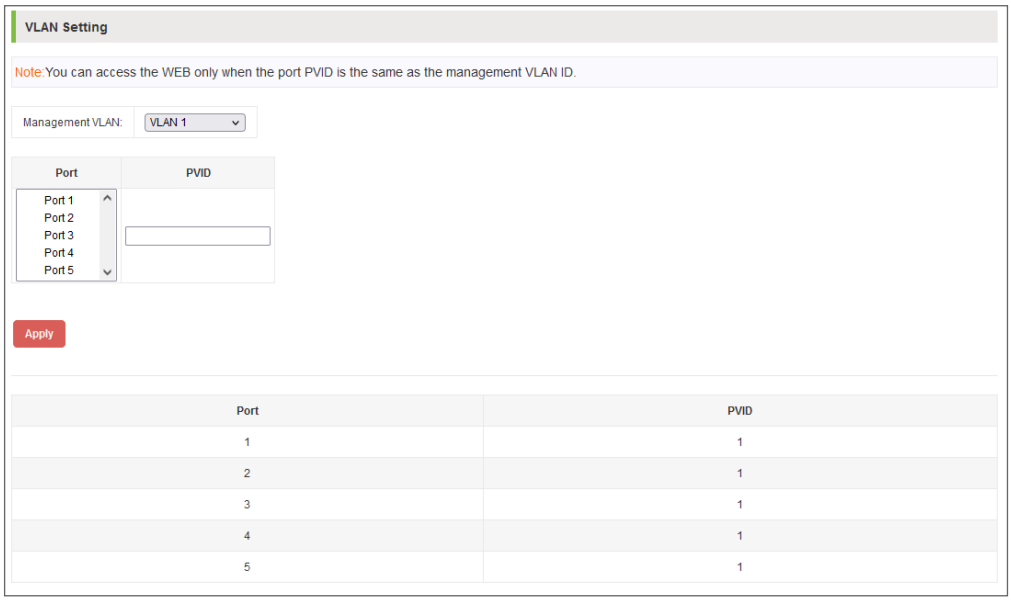
- **Management VLAN** — The VLAN that allows access to the switch web interface. (Default: 1)
- **Port** — Lists the switch port numbers.
- **PVID** — The VLAN ID assigned to untagged frames received on the port. (Default: 1

Web Interface

To configure a static VLAN:

1. Click VLAN, then VLAN Setting.
2. Select a VLAN ID for the Management VLAN.
3. Select one or more port numbers and configure the PVID.
4. Click Apply.

Figure 18: Configuring VLAN Settings



5 QoS Configuration

Quality of Service (QoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports QoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

This chapter describes the following topics:

- QoS Basic — Configures the priority queue mode and queue weight for ports.
- QoS Advanced — Configures the QoS Mode for incoming packets and maps QoS priorities to port priority queues.

QoS Basic

Use the QoS > QoS Basic page to set the queue mode for the egress queues on any port. The switch can be set to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before the lower priority queues are serviced, or Weighted Round-Robin (WRR) queuing which specifies a scheduling weight for each queue.

Usage Guidelines

- Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.
- WRR queuing specifies a relative weight for each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.
- A weight can be assigned to each of the weighted queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue is polled for service, and subsequently affects the response time for software applications assigned a specific priority value.
- The specified queue mode applies to all interfaces.

Parameters

These parameters are displayed:

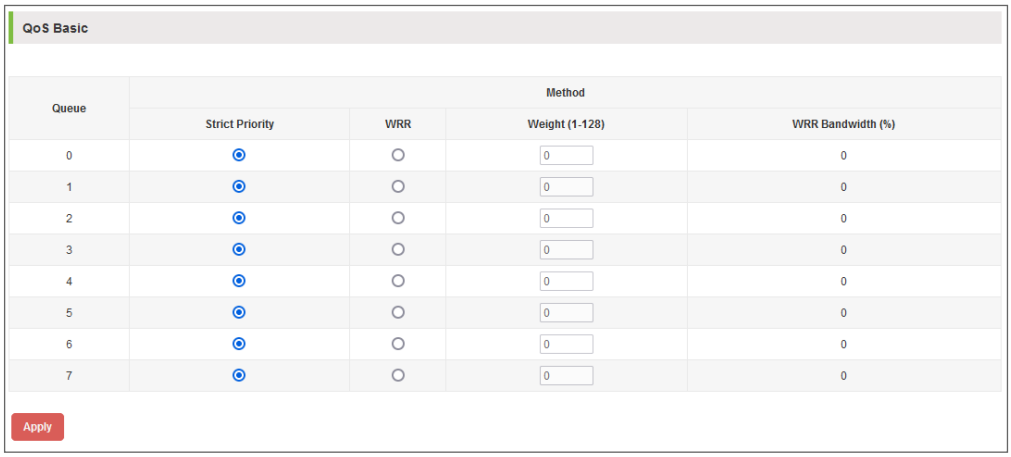
- **Queue** — The ID of the priority queue. (Range: 0-7)
- **Strict Priority** — Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic. (This is the default setting.)
- **WRR** — Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights, and servicing each queue in a round-robin fashion.
- **Weight** — Sets a weight for each queue which is used by the WRR scheduler. (Range: 1-128; Default: Weight of 0 (disabled) is assigned to queues 0 - 7)
- **WRR Bandwidth** — The percentage of bandwidth assigned to each queue based on the WRR weight.

Web Interface

To configure QoS priority queues:

1. Click QoS, then QoS Basic.
2. For each priority queue, select strict or WRR priority.
3. For queues using WRR priority, set a weight.
4. Click Apply.

Figure 19: Configuring QoS Basic



QoS Advanced

Use the QoS > QoS Advanced page to select between using port-based, 802.1p-based, or DSCP-based priority QoS modes, as well as mapping QoS priorities to port priority queues. The default QoS mode is 802.1p-based priority.

Port-Based Priority

Use the Port-Based QoS Mode page to specify the default port priority for each port on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

Usage Guidelines

- This switch provides eight priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage, but can be configured to process each queue in strict order.
- The default priority applies for an untagged frame received on a port. This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

Parameters

These parameters are displayed:

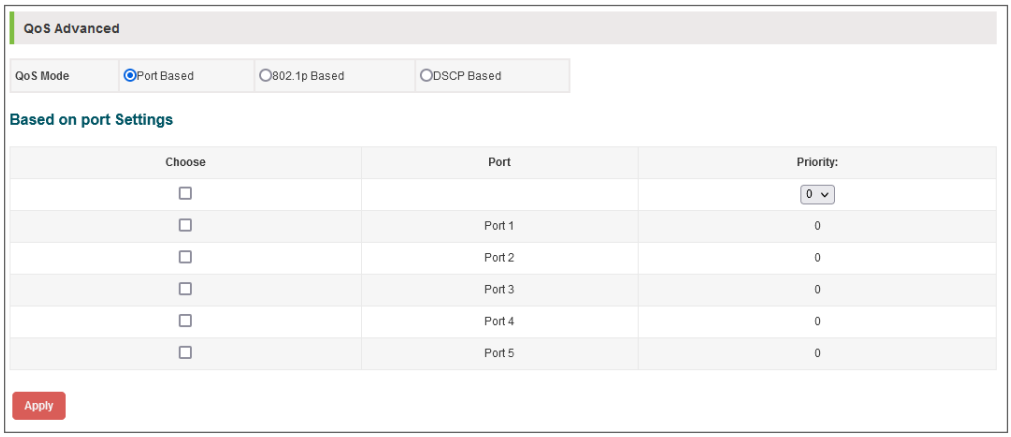
- **Port** — Displays a list of ports.
- **Priority** — The priority that is assigned to untagged frames received on the specified port. (Range: 0-7; Default: 0)

Web Interface

To configure QoS port-based priority:

1. Click QoS, then QoS Advanced.
2. Select Port Based for the QoS Mode.
3. For each port, select the QoS priority.
4. Click Apply.

Figure 20: Configuring Port-Based Priority



802.1p-Based Priority

Use the 802.1p-Based QoS Mode page to show the mapping of 802.1p priority values of incoming frames to internal priorities on the switch.

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in Table 2. However, priority levels can be mapped to the switch's output queues in any way that benefits application traffic for the network.

Table 2: QoS Priority Levels

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

Parameters

These parameters are displayed:

- **802.1p** — The QoS value in ingress packets. (Range: 0-7)
- **Priority** — The priority value used by the switch. (Range: 0-7)

Web Interface

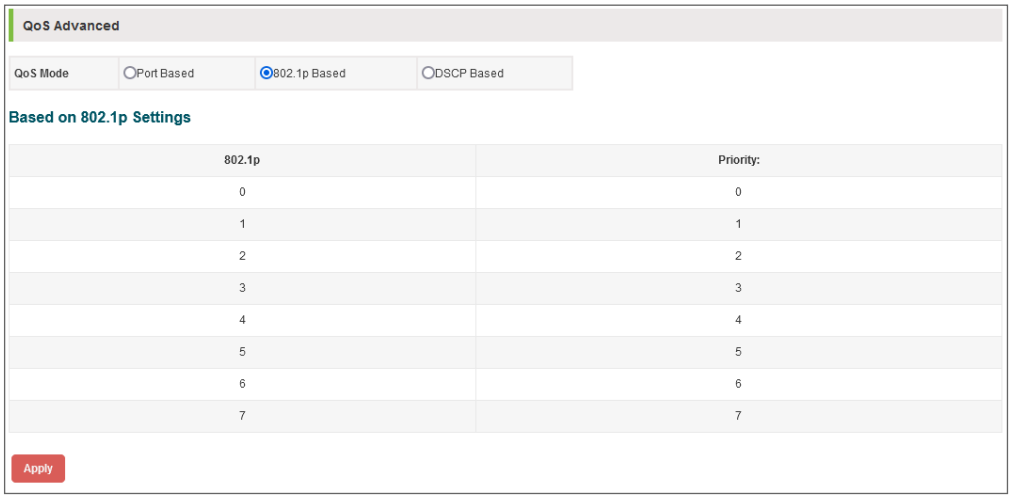
To configure QoS 802.1p-based priority:

1. Click QoS, then QoS Advanced.

2. Select 802.1p Based for the QoS Mode.

3. Click Apply.

Figure 21: Configuring 802.1p-Based Priority



DSCP-Based Priority

Use the DSCP-Based QoS Mode page to map DSCP values in incoming frames to QoS values for internal priority processing.

The switch supports a common method of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame using the six priority bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a QoS value by the switch, and the traffic then sent to the corresponding output queue.

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

Parameters

These parameters are displayed:

- **DSCP** — The DSCP value in ingress packets. (Range: 0-63)
- **Priority** — The priority value used by the switch. (Range: 0-7)

Web Interface

To configure DSCP-based priority:

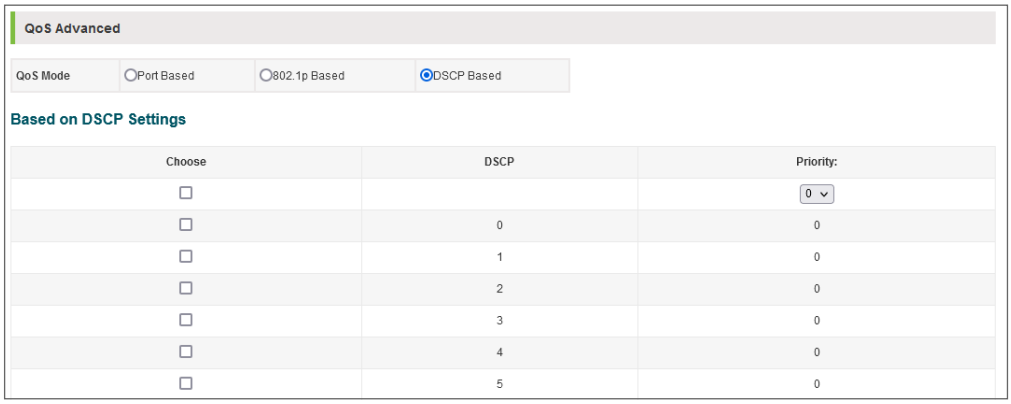
1. Click QoS, then QoS Advanced.

2. Select DSCP Based for the QoS Mode.

3. For each DSCP value, set a QoS priority value.

4. Click Apply.

Figure 22: Configuring DSCP-Based Priority



Priority Queue Mapping

Use the QoS > QoS Advanced page to map QoS values in packets to switch port priority queues.

Parameters

These parameters are displayed:

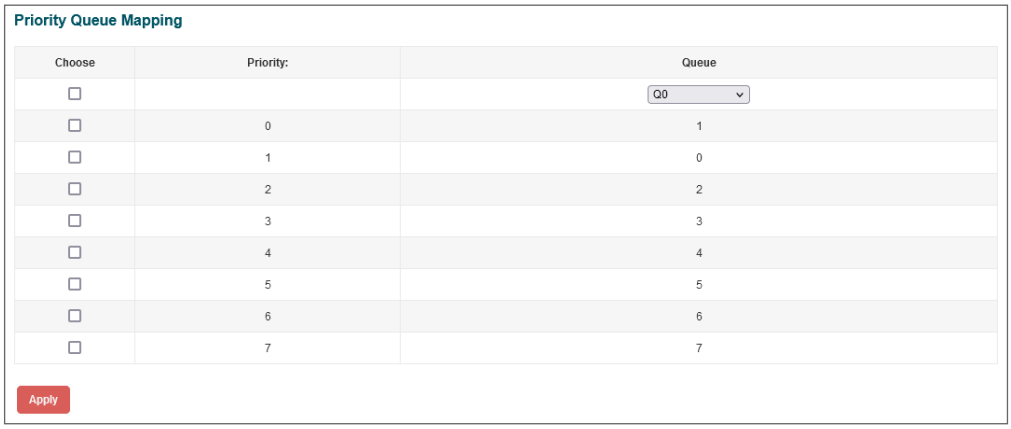
- **Priority** — The priority value used by the switch. (Range: 0-7)
- **Queue** — The output port priority queue. (Range: Q0-Q7)

Web Interface

To configure priority queue mapping:

1. Click QoS, then QoS Advanced.
2. For each QoS priority value, set a port priority queue.
3. Click Apply.

Figure 23: Configuring Priority Queue Mapping



6 PoE Configuration

The switch can provide DC power to a wide range of connected devices, eliminating the need for an additional power source and cutting down on the amount of cables attached to each device. Once configured to supply power, an automatic detection process is initialized by the switch that is authenticated by a PoE signature from the connected device.

The switch's power management enables individual port power to be controlled within the switch's power budget. Port power can be automatically turned on and off for connected devices. When a device is connected to a switch port, its power requirements are detected by the switch before power is supplied. If the power required by a device exceeds the power budget of the port or the whole switch, port power is not supplied.

This chapter describes the following topics:

- PoE Port Config — Enables PoE on ports and displays the status of connected devices.
- PoE System Power — Displays the current status of PoE power usage on the switch.
- PD Alive — Configures periodic checking of connected PoE powered devices.
- PoE Timer Rule — Configures daily time limits during which PoE power is available on ports.
- PoE Timer Set — Assigns configured timer rules to specific ports.
- PoE Extend Mode — Configures ports for a long-reach mode of operation where the transmission distance can be extended up to 250 meters.

PoE Port Config

Use the PoE > PoE Port Config page to enable PoE on ports and view the status of PoE power supplied to connected devices.

Usage Guidelines

- All the ECS1100 switches support the IEEE 802.3af PoE and IEEE 802.3at-2009 PoE+ standards. The ECS1100-10HP switch also supports the IEEE 802.3bt PoE++ standard on ports 1-4, and the ECS1100-28HP supports IEEE 802.3bt PoE++ on ports 1-8.

- The total PoE power delivered by all ports cannot exceed the maximum power budget of the switch. The maximum number of ports that can supply power simultaneously at the specified levels are shown in the following table.

Table 3: Maximum Number of Ports Providing Simultaneous Power

Maximum Port Power	ECS1100-5P Max Ports (Power Budget 120 W)	ECS1100-10HP Max Ports (Power Budget 250 W)	ECS1100-28HP Max Ports (Power Budget 480 W)
4 W (Class 1)	4	8	24
7 W (Class 2)	4	8	24
15.4 W (Class 3)	4	8	24
30 W (Class 4)	4	8	16
45 W (Class 5)	Not supported	4 (Ports 1-4 only)	8 (Ports 1-8 only)
60 W (Class 6)	Not supported	4 (Ports 1-4 only)	8 (Ports 1-8 only)
75 W (Class 7)	Not supported	3 (Ports 1-4 only)	6 (Ports 1-8 only)
90 W (Class 8)	Not supported	2 (Ports 1-4 only)	5 (Ports 1-8 only)

- If a device is connected to a switch port and the switch detects that it requires more than the switch power budget, no power is supplied to the device (i.e., port power remains off).

Parameters

These parameters are displayed:

- **Port** — Displays a list of ports.
- **Control** — Shows if PoE is enabled on a port. Power is automatically supplied when a device is detected on a port, providing that the power demanded does not exceed the switch or port power budget. (Default: Enabled)
- **State** — Status of the PoE power service provided to the switch port.
- **MaxPower** — Indicates that maximum port power is dependent on the connected powered device (PD) class.
- **Power** — The current power consumption on the port.
- **Voltage** — The voltage of the supplied power on the port.
- **Current** — The current of the supplied power on the port.
- **Class** — The detected power class of a connected device.

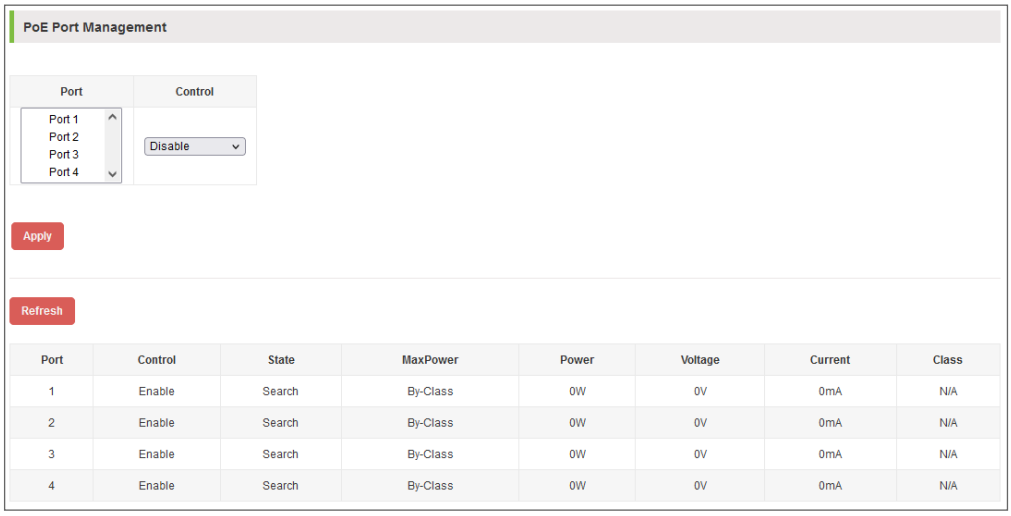
Web Interface

To enable or disable PoE on a port:

1. Click PoE, then PoE Port Config.

2. Select one or more ports in the Port list.
3. Set the Control to enable or disable.
4. Click Apply.

Figure 24: Configuring Port PoE



PoE System Power

Use the PoE > PoE System Power page to view the current status of PoE power usage on the switch.

Parameters

These parameters are displayed:

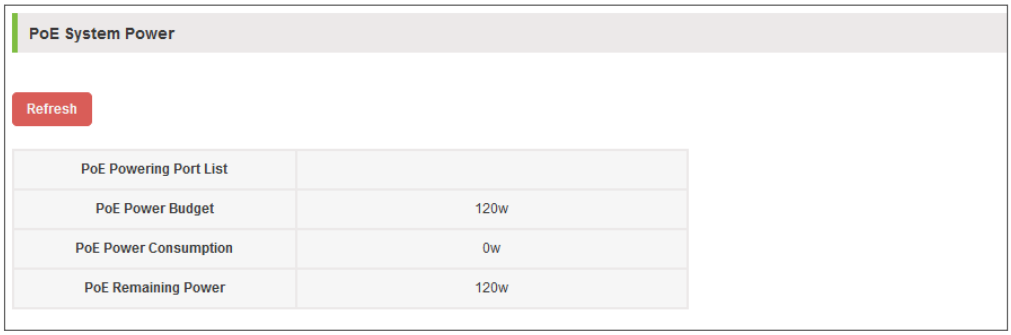
- **PoE Powering Port List** — The ports currently using PoE power.
- **PoE Power Budget** — The maximum PoE power available to all switch ports.
- **PoE Power Consumption** — The total PoE power currently being used by connected devices.
- **PoE Remaining Power** — The amount of PoE power still available within the switch power budget.

Web Interface

To display PoE system power information:

1. Click PoE, then PoE System Power.
2. Click Refresh to update the displayed information.

Figure 25: Displaying PoE System Power



PD Alive

Use the PoE > PD Alive page to configure periodic checking of connected PoE powered devices.

Parameters

These parameters are displayed:

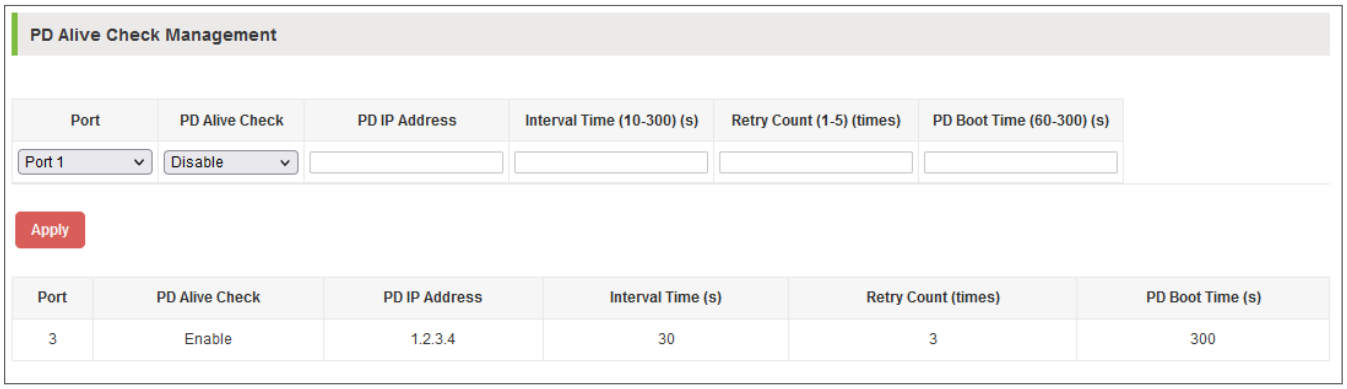
- **Port** — Selects a port number.
- **PD Alive Check** — Enables the periodic checking of connected powered devices to determine their alive status. (Default: Disabled for all ports)
- **PD IP Address** — The IPv4 address of the connected device.
- **Interval Time** — The time between each PD alive check. (Range: 10-300 seconds)
- **Retry Count** — The number of times a PD alive check is sent to a device before the device is reported as down. (Range: 1-5 times)
- **PD Boot Time** — The wait time before a device is restarted. (Range: 60-300 seconds)

Web Interface

To configure PD Alive checking:

1. Click PoE, then PD Alive.
2. Select the port that you want to configure or modify.
3. Set PD Alive Check to enable for the port.
4. Enter the PD IP Address, Interval Time, Retry Count, and PD Boot Time.
5. Click Apply.

Figure 26: Configuring PD Alive Management



PoE Timer Rule

Use the PoE > PoE Timer Rule page to configure daily time limits during which PoE power is available on ports.

Usage Guidelines

- PoE timer rules can be configured only after setting the system time.
- If a timer rule is set and applied to ports, then PoE will be provided to connected devices only during the specified period.
- Rules are assigned to ports using the PoE > PoE Timer Set page.

Parameters

These parameters are displayed:

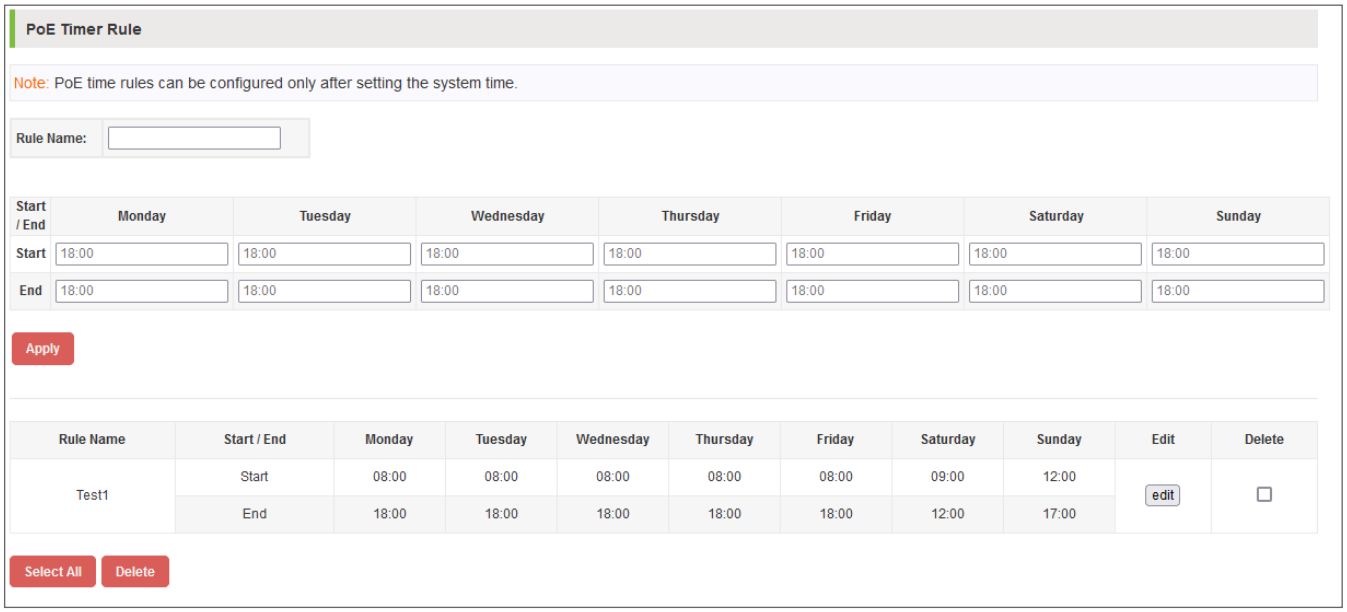
- **Rule Name** — A name that identifies the timer rule.
- **Start /End** — For each day of the week, specifies start and end times for PoE to be available on ports.
- **Edit/Delete** — Enables configured rules to be modified or deleted.

Web Interface

To configure PoE timer rules:

1. Click PoE, then PoE Timer Rule.
2. Define a name for the rule.
3. For each day of the week, set the start and end times for the rule.
4. Click Apply.

Figure 27: Configuring PoE Timer Rules



PoE Timer Set

Use the PoE > PoE Timer Set page to assign configured timer rules to specific ports.

Usage Guidelines

- PoE timer rules can only take effect after setting the system time.
- If a timer rule is set and applied to ports, then PoE will be provided to connected devices only during the specified period.
- Timer rules are configured using the PoE > PoE Timer Rule page.

Parameters

These parameters are displayed:

- **Port** — Displays a list of ports.
- **PoE Timer Rule** — A list of configured timer rules that can be selected.

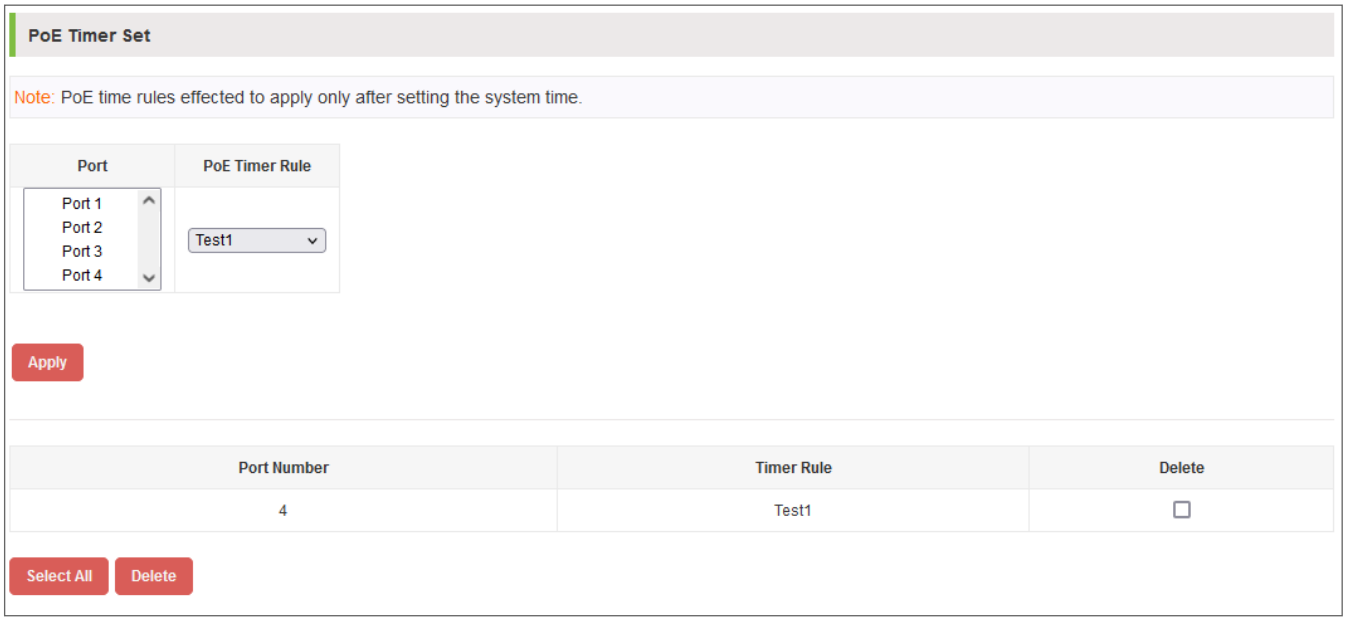
Web Interface

To assign PoE timer rules to ports:

1. Click PoE, then PoE Timer Set.
2. Select one or more ports from the Port list.
3. Select a timer rule from the PoE Timer Rule list.

4. Click Apply.

Figure 28: Assigning PoE Timer Rules to Ports



PoE Extend Mode

Use the PoE > PoE Extend Mode page to configure ports for a long-reach mode of operation where the transmission distance can be extended up to 250 meters.

Usage Guidelines

- PoE Extend Mode is only configurable for defined port groups. The port groups on the ECS1100 switches are:
  - ECS1100-5P: Ports 1-2 only
  - ECS1100-10HP: Ports 1-4, 5-8
  - ECS1100-28HP: Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24.
- When PoE Extend Mode is enabled on a port group, the transmission distance can be extended up to 250 meters. However, the network speed of the ports will be limited to 10 Mbps.
- PoE Extend Mode is suitable for installing devices that require low bandwidth, such as still cameras in remote places.
- If enabled for a port group and a group-related port is changed via Port Configuration, the port group will exit PoE Extend Mode automatically.

Parameters

These parameters are displayed:

- **Port Group** — Displays a list of port groups.
- **Extend Mode** — Enables the long-reach mode of operation for ports.

Web Interface

To enable PoE Extend Mode on port groups:

1. Click PoE, then PoE Extend Mode.
2. Select one or more port groups from the Port Group list.
3. Set Extend Mode to enabled.
4. Click Apply.

Figure 29: Enabling PoE Extend Mode on Port Groups

7 IGMP Configuration

This switch can use Internet Group Management Protocol (IGMP) to filter multicast traffic. IGMP Snooping can be used to passively monitor or "snoop" on exchanges between attached hosts and an IGMP-enabled device, most commonly a multicast router. In this way, the switch can discover the ports that want to join a multicast group, and set its filters accordingly.

This chapter describes the following topics:

- IGMP Snooping — Enables IGMP Snooping on the switch.
- Router Port — Configures ports that are attached to a multicast router/switch.
- Group Address — Statically assigns a multicast service to a port on the switch.

IGMP Snooping

Use the IGMP > IGMP Snooping page to enable the switch to forward multicast traffic efficiently to the attached network.

Usage Guidelines

- Based on the IGMP query and report messages, the switch forwards multicast traffic only to the ports that request it. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.
- This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. The switch simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.
- IGMP can be enabled on up to 2 VLANs simultaneously.

Parameters

These parameters are displayed:

- **IGMP Snooping Setting** — When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Disabled)

- **VLAN ID for IGMP Snooping** — Selects the VLAN which is to propagate all multicast traffic coming from the attached multicast router.

Web Interface

To enable or disable IGMP:

1. Click IGMP, then IGMP Snooping.
2. Set the IGMP Snooping Setting to Enable.
3. Select the VLAN on which IGMP Snooping will function.
4. Click Apply.

Figure 30: Enabling IGMP Snooping

Router Port

Use the IGMP > Router Port page to statically configure ports that are attached to a multicast router/switch.

Usage Guidelines

- Depending on network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to port on the switch, the port (and a specified VLAN) can be manually configured to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate ports within the switch.

- IGMP Snooping must be enabled on the switch before a multicast router port can be configured.

Parameters

These parameters are displayed:

- **Port** — Specifies a port attached to a multicast router.

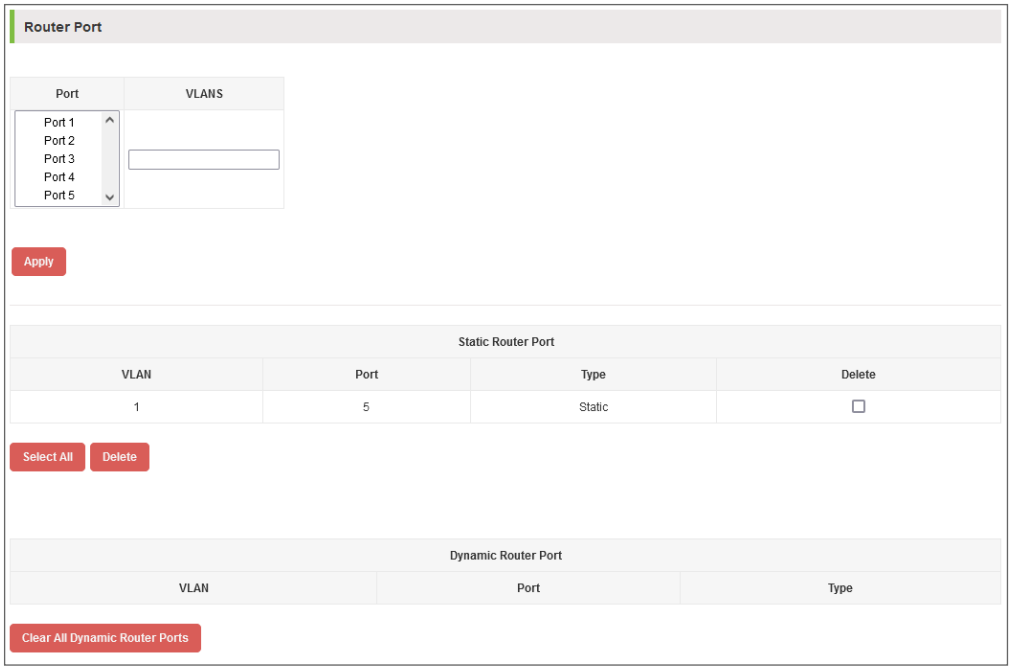
- **VLANs** — Selects the VLAN that is to propagate all multicast traffic coming from the attached multicast router. (Range: 1-4094)
- **Static Router Port** — Lists the VLAN, Port, and Type (static or dynamic) for configured router ports.
- **Dynamic Router Port** — Lists the VLAN, Port, and Type (static or dynamic) for router ports that have been dynamically discovered.

Web Interface

To configure static multicast router ports:

1. Click IGMP, then Router Port.
2. Select one or more ports from the Port list.
3. List the VLANs for which to display the multicast router port information.
4. Click Apply.

Figure 31: Configuring Static IGMP Router Ports



Group Address

Use the IGMP > Group Address page to statically assign a multicast service to a port on the switch.

Usage Guidelines

- Multicast filtering can be dynamically configured using IGMP Snooping, but in some cases it may be necessary to statically configure a multicast service on the switch. First, add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.
- Static multicast addresses are never aged out.
- When a multicast address is assigned to a port in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Parameters

These parameters are displayed:

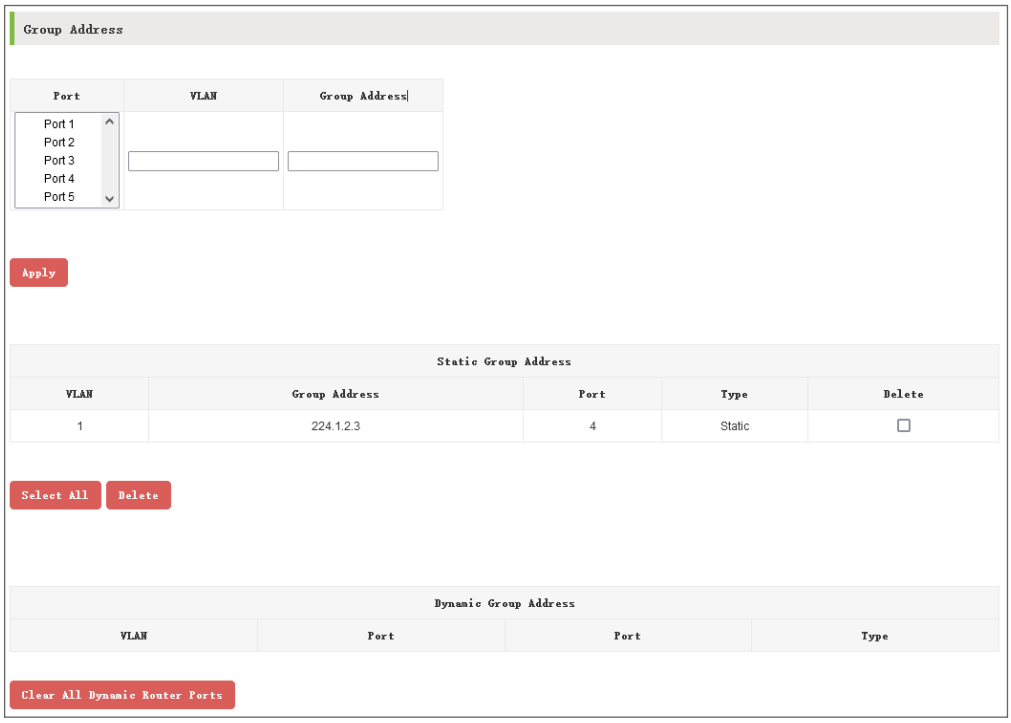
- **Port** — Specifies the ports assigned to a multicast group.
- **VLANs** — Specifies the VLAN which is to propagate the multicast service. (Range: 1-4094)
- **Group Address** — The IPv4 address for a specific multicast service.

Web Interface

To statically assign a port to a multicast service:

1. Click IGMP, then Group Address.
2. Select one or more ports from the Port list.
3. Specify the VLAN that will propagate the multicast service.
4. In the Group Address field, enter the multicast IP address.
5. Click Apply.

Figure 32: Configuring Static Multicast Group Addresses



8 Tools

The switch provides tools for upgrading the system software, backing up and restoring the configuration, resetting the switch to factory defaults, and restarting the switch.

This chapter describes the following topics:

- System Upgrade — Upgrades the switch operating software.
- Backup Restore — Saves the current switch configuration, backs up the configuration file, and restores a previously saved configuration.
- System Reset — Resets the switch configuration to factory defaults and restarts the system.
- System Reboot — Restarts the switch.

System Upgrade

Use the Tools > System Upgrade page to upgrade the switch operating software with a file provided by Edgecore.

Usage Guidelines

- You need to restart the switch after the upgrade is complete.
- Do not power off the switch during the upgrade process, otherwise the switch may be damaged.
- It is recommended to backup the current configuration before upgrading.

Parameters

These parameters are displayed:

- **Select File** — Selects a system software file stored on the management station.
- **Upload** — Uploads the new software file to the switch.

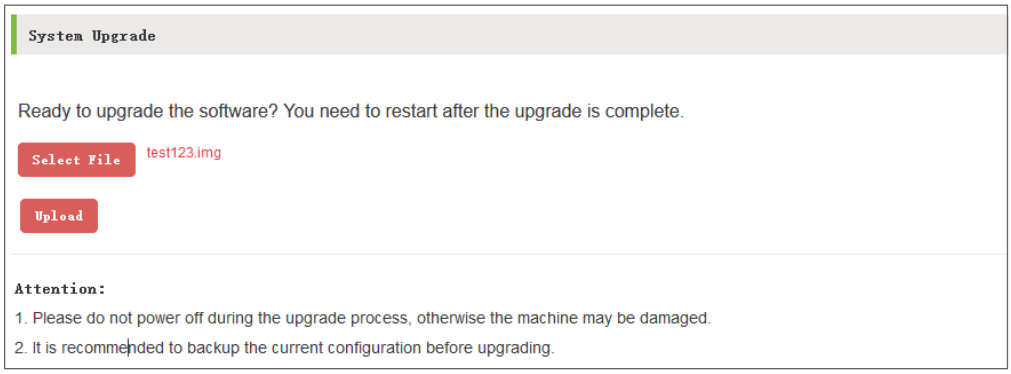
Web Interface

To upgrade the switch's system software:

1. Click Tools, then System Upgrade.

2. Click the Select File button and locate the upgrade file.
3. Click the Upload button.
4. When the upgrade is complete, reboot the switch.

Figure 33: Upgrading the System Software



Backup Restore

Use the Tools > Backup Restore page to save the current switch configuration, backup the configuration file, and restore a previously saved configuration.

Usage Guidelines

- The switch configuration settings are not automatically saved by the system for subsequent use when the switch is rebooted. You must save these settings to a configuration file on the switch.
- It is recommended to save the current configuration before backing up.
- It can take a few minutes to back up or restore the configuration. Do not perform other operations during this period.
- Do not power off during a backup or restore operation, otherwise the switch may be damaged.
- The current configuration is lost when you restore a previous configuration. An incorrect configuration may cause the switch to be unmanageable.

Parameters

These parameters are displayed:

- **Save** — Saves the current configuration to a file on the switch.
- **Configuration Backup** — Downloads the configuration file to the management station.

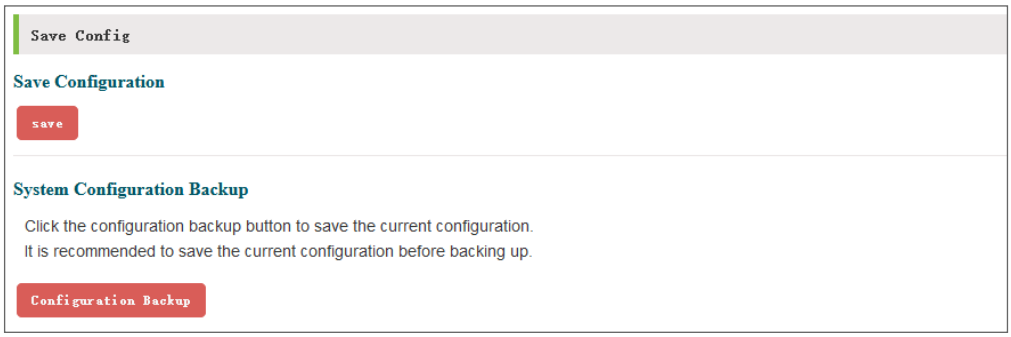
- **Select File** — Selects a previously saved configuration file stored on the management station.
- **Configuration Restore** — Uploads a configuration file and replaces the current switch configuration.

Web Interface

To backup a switch configuration:

1. Click Tools, then Backup Restore.
2. Click Save to save the current running configuration.
3. Click Configuration Backup.

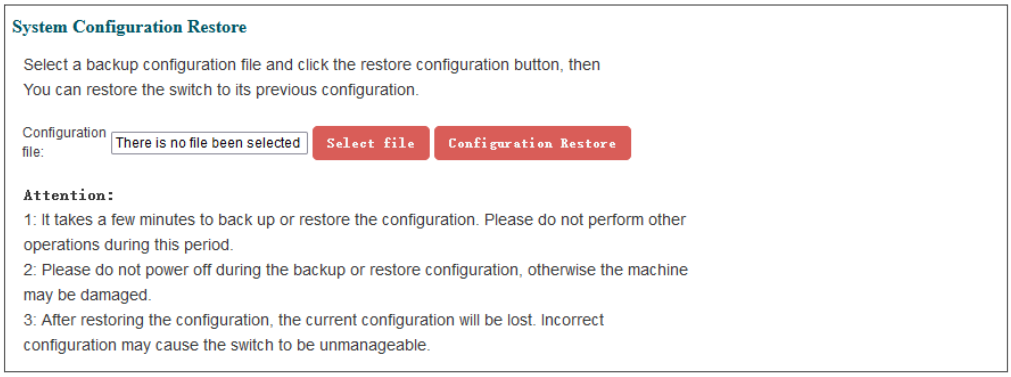
Figure 34: Backing Up the Switch Configuration



To restore a switch configuration:

1. Click Tools, then Backup Restore.
2. Click Select File and locate the configuration file to restore.
3. Click Configuration Restore.

Figure 35: Restoring the Switch Configuration



System Reset

Use the Tools > System Reset page to reset the switch configuration to factory defaults and restart the system.

Usage Guidelines

- The reset operation resets the entire switch system.
- It can take a few minutes to reset the switch. Do not try to perform other operations or power off the switch during this period.

Parameters

These parameters are displayed:

- **Reset** — Resets the configuration and restarts the system immediately.

Web Interface

To reset the switch configuration to factory defaults:

1. Click Tools, then System Reset.
2. Click Reset to restore factory default settings and restart the system.
3. When prompted, confirm that you want to reset the switch.

Figure 36: Resetting the Switch to Factory Default Settings

System Reboot

Use the Tools > System Reboot page to restart the system.

Usage Guidelines

- The reboot operation prompts to save the current configuration. When the system is restarted, it retains the last saved configuration.
- It can take a few minutes to reboot the switch. Do not try to perform other operations or power off the switch during this period.

Parameters

These parameters are displayed:

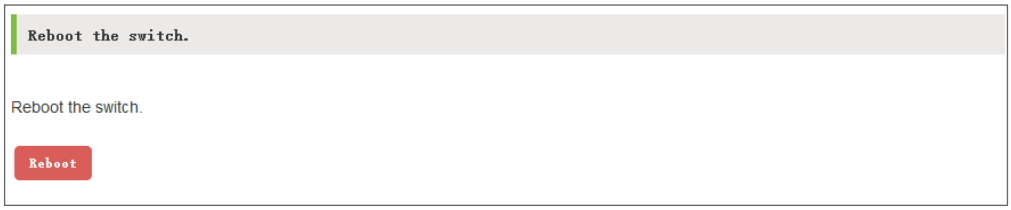
- **Reboot** — Restarts the system immediately.

Web Interface

To restart the switch:

1. Click Tools, then System Reboot.
2. Click Reboot to restart the system.
3. When prompted, confirm that you want to reboot the switch.
4. When prompted, confirm that you want save the current switch configuration.

Figure 37: Rebooting the Switch



Section III

Appendices

This section provides additional information and includes these items:

A Troubleshooting

Problems Accessing the Management Interface

Table 4: Troubleshooting Chart

Symptom	Action
Cannot connect using a web browser	■ Be sure the device is powered up. ■ Check that you have a valid network connection to the switch and that the port you are using has not been disabled. ■ Be sure you have configured the management VLAN through which the management station is connected with a valid IP address, subnet mask and default gateway. ■ Be sure the management station has an IP address in the same subnet as the switch. ■ Be sure you have set up accounts on the device for each user, including user names and passwords.
Forgot or lost the password	■ Press and hold the reset button on the front of the switch for about 10 seconds to reset to factory defaults.

B License Information

This product includes copyrighted third-party software subject to the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other related free software licenses. The GPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, refer to the section "The GNU General Public License" below, or refer to the applicable license as included in the source-code archive.

The GNU General Public License

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS