Status and Statistics

This chapter contains the following sections:

System Summary

The System Summary provides a preview of the device status, hardware, firmware version, general PoE status, and other system information.

To view the system information, click **Status and Statistics** > **System Summary**.

System Information

The System Information section provides a quick way to get information about your device. In this section, you will be able to see the following information:

- System Description—A description of the system.
- System Location—Physical location of the device. Click **Edit** to go System Settings to enter this value.
- System Contact—Name of a contact person. Click **Edit** to go System Settings to enter this value.

- Host Name—Name of the device. Click **Edit** to go System Settings to enter this value. By default, the device host name is composed of the word switch concatenated with the three least significant bytes of the device MAC address (the six furthest right hexadecimal digits).
- System Object ID—Unique vendor identification of the network management subsystem contained in the entity (used in SNMP).
- System Uptime—Time that has elapsed since the last reboot.

Note For the System Uptime, the time counter will reset after 497 days.

- Current Time—Current system time.
- Base MAC Address—Device MAC address.
- Jumbo Frames—Jumbo frame support status. This support can be enabled or disabled by using the Port Settings.

Note Jumbo frames support takes effect only after it is enabled, and after the device is rebooted.

Software Information:

- Firmware Version (Active Image)—Firmware version number of the active image.

Note In a stack, the Firmware Version number shown is based on the version of the active unit.

- Firmware MD5 Checksum (Active Image)—MD5 checksum of the active image.
- Firmware Version (Non-active)—Firmware version number of the non-active image. If the system is in a stack, the version of the active unit is displayed.
- Firmware MD5 Checksum (Non-active)—MD5 checksum of the non-active image.

Note If you loaded language(s) on the device, the following fields show the attributes of the language(s).

- Locale—Locale of the language.
- Language Version—Language package version of the language.

TCP/UDP Services Status

To reset the following fields, click **Edit** to open TCP/UDP Services.

- HTTP Service—Whether HTTP is enabled/disabled.
- HTTPS Service—Whether HTTPS is enabled/disabled.
- SNMP Service—Whether SNMP is enabled/disabled.
- Telnet Service—Whether Telnet is enabled/disabled.
- SSH Service—Whether SSH is enabled/disabled.

PoE Power Information on Device Supporting PoE

The PoE Power Information on Device Supporting PoE section provides a quick way to get PoE information on your device. In this section, the following will be displayed:

- PoE Power Information—Click on Detail to display the PoE power information.
- Maximum Available PoE Power (W)—Maximum available power that can be delivered by the switch.
- Total PoE Power Allocated (W)—Total PoE power allocated to connected PoE devices.
- PoE Power Mode—Port Limit or Class Limit.

The unit is displayed graphically, and hovering on a port displays its name.

The following information is displayed for each unit:

- Unit #— Device model ID.
- Serial Number—Serial number.

CPU Utilization

The device CPU handles the following types of traffic, in addition to end-user traffic handling the management interface:

- Management traffic
- Protocol traffic
- Snooping traffic

Excessive traffic burdens the CPU, and might prevent normal device operation. The device uses the Secure Core Technology (SCT) to ensure that the device receives and processes management and protocol traffic. SCT is enabled by default on the device and can’t be disabled.

To display CPU utilization, follow these steps:

Step 1 Click **Status and Statistics** > **CPU Utilization**.

The CPU Input Rate field displays the rate of input frames to the CPU per second. The window contains a graph displaying CPU utilization on the device. The Y axis is percentage of usage, and the X axis is the sample number.

Step 2 Check **Enable** to enable the CPU Utilization.

Step 3 Select the Refresh Rate (time period in seconds) that passes before the statistics are refreshed. A new sample is created for each time period.

The window containing a graph displaying CPU utilization on the device is displayed.

Port Utilization

The Port Utilization page displays utilization of broadband (both incoming and outgoing) per port.

To display port utilization, follow these steps:

Step 1 Click **Status and Statistics** > **Port Utilization**.

Step 2 Enter the **Refresh Rate**, which is the time period that passes before the interface Ethernet statistics are refreshed.

The following fields are displayed for each port:

- Interface—Name of port.
- Tx Utilization—Amount of bandwidth used by outgoing packets.
- Rx Utilization—Amount of bandwidth used by incoming packets.

To view a graph of historical utilization over time on the port, select a port and click View Interface History Graph. In addition to the above, the following field is displayed:

- Time Span—Select a unit of time. The graph displays the port utilization over this unit of time.

Interface

The Interface page displays traffic statistics per port. This page is useful for analyzing the amount of traffic that is both sent and received, and its dispersion (Unicast, Multicast, and Broadcast).

To display Ethernet statistics and/or set the refresh rate, follow these steps:

Step 1 Click **Status and Statistics** > **Interface**.

Step 2 To view statistics counters in table view or graphic view:

- Click **Clear Interface Counters**, to clear all counters.
- Click **Refresh** to refresh the counters.
- Click **View All Interfaces Statistics** to see all ports in table view.

- Click **View Interface History Graph** to display these results in graphic form. Select the **Interface** to view the the statistics pertaining to that interface.

Step 3 Enter the parameters.

- Interface—Select the interface for which Ethernet statistics are to be displayed.
- Refresh Rate—Select the time period that passes before the interface Ethernet statistics are refreshed.

Step 4 In the Receive Statistics section, the following stats are displayed:

- Total Bytes (Octets)—Octets received, including bad packets and FCS octets, but excluding framing bits.
- Unicast Packets—Good Unicast packets received.
- Multicast Packets—Good Multicast packets received.
- Broadcast Packets—Good Broadcast packets received.
- Packets with Errors—Packets with errors received.

Step 5 In the Transmit Statistics section, the following stats are displayed:

- Total Bytes (Octets)—Octets transmitted, including bad packets and FCS octets, but excluding framing bits.
- Unicast Packets—Good Unicast packets transmitted.
- Multicast Packets—Good Multicast packets transmitted.
- Broadcast Packets—Good Broadcast packets transmitted.

Etherlike

The Etherlike page displays statistics per port according to the Etherlike MIB standard definition. The refresh rate of the information can be selected. This page provides more detailed information regarding errors in the physical layer (Layer 1) that might disrupt traffic.

To view Etherlike Statistics and/or set the refresh rate follow these steps:

Step 1 Click **Status and Statistics** > **Etherlike**.

Step 2 Enter the parameters.

- Interface—Select the specific interface for which Ethernet statistics are to be displayed.
- Refresh Rate—Select the amount of time that passes before the Etherlike statistics are refreshed.

The fields are displayed for the selected interface.

- Frame Check Sequence (FCS) Errors — Received frames that failed the CRC (cyclic redundancy checks).
- Single Collision Frames— Frames that involved in a single collision, but successfully transmitted.

- Late Collisions—Collisions that have been detected after the first 512 bits of data.
- Excessive Collisions—Transmissions rejected due to excessive collisions.
- Oversize Packets—Packets greater than 2000 octets received.
- Internal MAC Receive Errors—Frames rejected because of receiver errors.
- Pause Frames Received— Displays the number of frames received.
- Pause Frames Transmitted—Displays the number of frames transmitted.

Note If one of the fields listed above shows a number of errors (not 0), a Last Up time is displayed.

Step 3 To view statistics counters in table view, click **View All Interfaces Statistics** to see all ports in table view. You can also click **Refresh** to refresh the stats or click **Clear Interface Counters** to clear the counters.

GVRP

The GARP VLAN Registration Protocol (GVRP) page displays the GVRP frames that are sent or received from a port. GVRP is a standards-based Layer 2 network protocol, for automatic configuration of VLAN information on switches. It is defined in the 802.1ak amendment to 802.1Q-2005. GVRP statistics for a port are only displayed if GVRP is enabled globally and on the port.

To view GVRP statistics and/or set the refresh rate, proceed as follows:

Step 1 Click **Status and Statistics** > **GVRP**.

Step 2 Enter the parameters.

Interface	Select the specific interface for which GVRP statistics are to be displayed.
Refresh Rate	Select the time period that passes before the GVRP page is refreshed. The Attribute Counter block displays the counters for various types of packets per interface. These are displayed for Received and Transmitted packets.

The Attribute Counter block displays the counters for various types of packets per interface. These are displayed for Received and Transmitted packets.

Join Empty	GVRP Join Empty packets received/transmitted.
Empty	GVRP empty packets received/transmitted
Leave Empty	GVRP Leave Empty packets received/transmitted.
Join In	GVRP Join In packets received/transmitted.
Leave In	GVRP Leave In packets received/transmitted.
Leave All	GVRP Leave All packets received/transmitted. The GVRP Error Statistics section displays the GVRP error counters.

The GVRP Error Statistics section displays the GVRP error counters.

Invalid Protocol ID	Invalid protocol ID errors.
Invalid Attribute Type	Invalid attribute ID errors.
Invalid Attribute Value	Invalid attribute value errors.
Invalid Attribute Length	Invalid attribute length errors.
Invalid Event	Invalid events.

Step 3 To clear statistics counters, click **View All Interfaces Statistics** to see all ports on a single page.

802.1X EAP

The 802.1x EAP page displays the Extensible Authentication Protocol (EAP) frames that are sent or received. To view the EAP Statistics and/or set the refresh rate, proceed as follows:

Step 1 Click **Status and Statistics** > **802.1x EAP**.

Step 2 Select the Interface that is polled for statistics.

Step 3 Select the Refresh Rate (time period) that passes before the EAP statistics are refreshed.

The values are displayed for the selected interface.

The values are displayed for the selected interface.

EAPOL EAP Frames Received	Valid EAPOL frames received on the port.
EAPOL Start Frames Received	Valid EAPOL start frames received on the port.
EAPOL Logoff Frames Received	EAPOL Logoff frames received on the port.
EAPOL Announcement Frames Received	EAPOL Announcement frames received on the port.
EAPOL Announcement Request Frames Received	EAPOL Announcement Request frames received on the port.
EAPOL Invalid Frames Received	EAPOL invalid frames received on the port.
EAPOL EAP Length Error Frames Received	EAPOL frames with an invalid Packet Body Length received on this port.
MKPDU Frames with unrecognized CKN Received	EAP frames with unrecognized CKN received on this port.
MKPDU Invalid Frames Received	MKPDU invalid frames received on the port.
Last EAPOL Frame Version	Protocol version number attached to the most recently received EAPOL frame.

Last EAPOL Frame Source	Source MAC address attached to the most recently received EAPOL frame.
EAPOL EAP Supplicant Frames Transmitted	EAPOL EAP Supplicant frames transmitted on the port.
EAPOL Start Frames Transmitted	EAPOL Start frames transmitted on the port.
EAPOL Logoff Frames Transmitted	EAPOL Logoff frames transmitted on the port.
EAPOL Announcement Frames Transmitted	EAPOL Announcement frames transmitted on the port.
EAPOL Announcement Request Frames Transmitted	EAPOL Announcement Request frames transmitted on the port.
EAPOL EAP Authenticator Frames Transmitted	EAP Authenticator frames transmitted on the port.
EAPOL MKA Frames with No CKN Transmitted	MKA frames with no CKN transmitted on the port.

Step 4 To clear statistics counters:

- Click **Clear Interface Counters** to clear the counters of all interfaces.
- Click **Refresh** to refresh the counters.
- Click **View All Interfaces Statistics** to view the counters of all interfaces.

ACL

When the ACL logging feature is enabled, an informational SYSLOG message is generated for packets that match ACL rules. To view the interfaces on which packets are forwarded or rejected based on ACLs, follow these steps:

Step 1 Click **Status and Statistics** > **ACL**.

Step 2 Select the Refresh Rate (time period in seconds) that passes before the page is refreshed. A new group of interfaces is created for each time period.

The following information is displayed:

- Global Trapped Packet Counter—Number of packets trapped globally due to lack of resources.
- Trapped Packets - Port/LAG Based—The interfaces on which packets forwarded or rejected based on ACL rules.
- Trapped Packets - VLAN Based—The VLANs on which packets forwarded or rejected based on ACL rules.

Step 3 To clear statistics counters, click **Clear Counters** or click **Refresh** to refresh the counters.

Hardware Resource Utilization

This page displays the resources used by the device, such as Access Control Lists (ACL) and Quality of Service (QoS). Some applications allocate rules upon their initiation. Also, processes that initialize during the system boot use some of their rules during the startup process.

To view the hardware resource utilization, click **Status and Statistics** > **Hardware Resource Utilization**.

The following fields are displayed:

- Unit No—Unit in stack for which TCAM utilization appears. This is not displayed when the device is in not part of a stack.
- IP Entries
  - In Use—Number of TCAM entries used for IP rules.
  - Maximum—Number of available TCAM entries that can be used for IP rules.
- IPv4 Policy Based Routing
  - In Use—Number of router TCAM entries used for IPv4 Policy-based routing
  - Maximum—Maximum number of available router TCAM entries that can be used for IPv4 Policy-based routing.
- IPv6 Policy Based Routing
  - In Use—Number of router TCAM entries used for IPv6 Policy-based routing
  - Maximum—Maximum number of available router TCAM entries that can be used for IPv6 Policy-based routing.
- VLAN Mapping
  - In Use—Number of router TCAM entries currently used for VLAN mapping
  - Maximum—Maximum number of available router TCAM entries that can be used for VLAN mapping.
- ACL and QoS Rules
  - In Use—Number of TCAM entries used for ACL and QoS rules
  - Maximum—Number of available TCAM entries that can be used for ACL and QoS rules.

Health and Power

The Health and Power page monitors the temperature, power supply, and fan status on all relevant devices. The fans on the device vary based on the model.

Environmental Status

- Fan Status—Displays whether the fan is operating normally (OK) or not (Failure).
- Redundant Fan Status— Displays the redundant status of the fan:
  - Ready—Redendant fan is operational but not required
  - Active—One of the main fans is not working and this fan is replacing it.
- Sensor Status—Displays whether the sensor is functional (OK) or not functional (Failure).
- Temperature—Displays one of the following options:
  - OK—The temperature is below the warning threshold.
  - Warning—The temperature is between the warning threshold to the critical threshold.
  - Critical—Temperature is above the critical threshold.
  - N/A—Not relevant.
- Main Power Status (these fields are found on device that are PD devices and in devices that support RPS)
- Main Power Supply Status—Displays the one of the following for the main power supply.
  - Active—Power supply is being used.
  - Failure—Main power has failed.

Power Savings

- Current Green Ethernet and Port Power Savings—Current amount of the power savings on all the ports.
- Cumulative Green Ethernet and Port Power Savings—Accumulative amount of the power savings on all the ports since the device was powered up.
- Projected Annual Green Ethernet and Port Power Savings—Projection of the amount of the power that will be saved on the device during one week. This value is calculated based on the savings that occurred during the previous week.
- Current PoE Power Savings (available for PoE SKUs only)—Current amount of the PoE power saved on ports that have PDs connected to them and on which PoE is not operational due to the Time Range feature.
- Cumulative PoE Power Savings (available for PoE SKUs only)—Cumulative amount of the PoE power, since the device was powered up, saved on ports which have PDs connected to them and to which PoE is not operational due to the Time Range feature.
- Projected Annual PoE Power Savings (available for PoE SKUs only)—Yearly projected amount of PoE power, since device was powered up, saved on ports that have PDs connected to them and to which PoE is not operational due to the Time Range feature. The projection is based on the savings during the previous week.

SPAN and RSPAN

The SPAN feature, which is sometimes called port mirroring or port monitoring, selects network traffic for analysis by a network analyzer. The network analyzer can be a Cisco Switch Probe device or other Remote Monitoring (RMON) probes.

Port mirroring is used on a network device to send a copy of network packets, seen on a single device port, multiple device ports, or an entire VLAN, to a network monitoring connection on another port on the device. This is commonly used when monitoring of network traffic, such as for an intrusion-detection system, is required. A network analyzer, connected to the monitoring port, processes the data packets. A packet, which is received on a network port and assigned to a VLAN that is subject to mirroring, is mirrored to the analyzer port even if the packet was eventually trapped or discarded. Packets sent by the device are mirrored when Transmit (Tx) mirroring is activated.

Mirroring does not guarantee that all traffic from the source port(s) is received on the analyzer (destination) port. If more data is sent to the analyzer port than it can support, some data might be lost.

VLAN mirroring cannot be active on a VLAN that was not manually created. For example, if VLAN 23 was created by GVRP, port mirroring will not work on it.

RSPAN

RSPAN extends SPAN by enabling monitoring of multiple switches across your network and allowing the analyzer port to be defined on a remote switch. In addition to the start (source) and final (destination) switches, you can define intermediate switches over which the traffic flows. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The traffic from the source interfaces on the start device is copied to the RSPAN VLAN through a reflector port and then forwarded over trunk ports on the intermediate devices to the destination session on the final switch, which is monitoring the RSPAN VLAN. The reflector port is the mechanism that copies packets to an RSPAN VLAN. It is a network port that handles various types of traffic. The RSPAN VLAN must be configured on all the intermediate switches.

Note RSPAN does not always successfully copy all the packets when they are arrive from multiple sources simultaneously. If accurate monitoring is required, the TCAM-based mirror policy can be used.

Start Switch

1. Define the RSPAN VLAN. This RSPAN VLAN must be the same in all switches.
2. Define one or more source interfaces, which can be ports or a VLAN, and ensure that it is not a member of the RSPAN VLAN.
3. Define a reflector port (destination, egress port) and ensure that it is not a member of the RSPAN VLAN.
4. Define the Destination Type as Remote VLAN.
5. Set Network Traffic to Enable.

Intermediate Switch(es)

1. Define the RSPAN VLAN. This RSPAN VLAN must be the same in the start, intermediate and final switches

2. Ensure that there are at least two ports that are members of the RSPAN VLAN. Traffic will pass through the switch via the RSPAN VLAN.

Final Switch

1. Define the RSPAN VLAN. This RSPAN VLAN must be the same in the start, intermediate and final switches.
2. Ensure that the source port, which is connected to the intermediate switch, is a member of the RSPAN VLAN.
3. Define the Source Interface as Remote VLAN.
4. Define a destination port and make sure it is not in the RSPAN VLAN.
5. Define the Destination Type as Local Interface.

RSPAN VLAN

An RSPAN VLAN carries SPAN traffic between RSPAN source and destination sessions and must be defined on the start, intermediate and final devices.

To configure a VLAN as an RSPAN VLAN, follow these steps:

Step 1 Click **Status and Statistics** > **SPAN & RSPAN** > **RSPAN VLAN.** to view the previously defined RSPAN VLAN.

Step 2 To configure a VLAN as a RSPAN VLAN, select it from the RSPAN VLAN drop-down list of VLANs.

Step 3 Click **Apply**.

Session Destinations

A monitoring session consists of one or more source ports and a single destination ports. A destination port must be configured on the start and final devices. On the start device, this is the reflector port. On the final device, it is the analyzer port.

To add a destination port, follow these steps:

Step 1 Click **Status and Statistics >SPAN & RSPAN> Session Destinations**.

Step 2 Click **Add**.

Step 3 Enter the following fields:

- Session ID—Select a session ID. This must match the session IDs of the source ports.
- Destination Type—Select one of the following options:
  - Local Interface—Is the destination port on the same device as the source ports (relevant to SPAN).
  - Remote VLAN—Is the destination port on a different device than the source port (relevant to RSPAN).

  If the Destination Type is Remote VLAN, configure the following field:
  - Reflector Port—Select a unit/port that functions as a target port on the first device.

If the Destination Type is Local Interface, configure the following field:

- Network Traffic—Select to enable that traffic other than monitored traffic is possible on the port.

Step 4 Click **Apply**.

Session Sources

In a single local SPAN or RSPAN session source, you can monitor the port traffic, such as received (Rx), transmitted (Tx), or bidirectional (both). The switch supports any number of source ports (up to the maximum number of available ports on the switch) and any number of source VLANs.

Note One or more SPAN or RSPAN sources must be configured on the start and final devices.

To configure the source ports to be mirrored, follow these steps:

Step 1 Click **Status and Statistics** > **SPAN & RSPAN** > **Session Sources**.

Step 2 Click **Add**.

Step 3 Select the session number from Session ID. This must be the same for all source ports and the destination port.

Step 4 For SPAN or for RSPAN on the start switch, select the unit and port or VLAN from which traffic is monitored (Source Interface). On the final switch, for RSPAN, select Remote VLAN

Step 5 In the **Monitor Type** field, select whether incoming, outgoing, or both types of traffic are mirrored.

- Rx and Tx—Port mirroring on both incoming and outgoing packets
- Rx—Port mirroring on incoming packets
- Tx—Port mirroring on outgoing packets

Step 6 Click **Apply**. The source interface for the mirroring is configured.

Diagnostics

You can use diagnostics to test and verify the functionality of the hardware components of your system (chassis, supervisor engines, modules, and ASICs) while your device is connected to a live network. Diagnostics consists of packet-switching tests that test hardware components and verify the data path and control signals.

Copper Test

The Copper Test page displays the results of integrated cable tests performed on copper cables by the Virtual Cable Tester (VCT).

VCT performs two types of tests:

- Time Domain Reflectometry (TDR) technology tests the quality and characteristics of a copper cable attached to a port. Cables of up to 140 meters long can be tested. These results are displayed in the Test Results block of the Copper Test page.
- DSP-based tests are performed on active XG links to measure cable length. These results are displayed in the Advanced Information block of the Copper Test page. This test can run only when the link speed is 10G.

Preconditions to Running the Copper Test

Before running the test, do the following:

- (Mandatory) Disable Short Reach mode (see Properties).
- (Optional) Disable EEE (see Properties).

Use a CAT6a data cable when testing cables using (VCT).

The test results have an accuracy within an error range of +/- 10 for advanced Testing and +/-2 for basic testing.

Caution When a port is tested, it is set to the Down state and communications are interrupted. After the test, the port returns to the Up state. It is not recommended that you run the copper port test on a port you are using to run the web-based switch configuration utility, because communications with that device are disrupted.

To test copper cables attached to ports:, follow these steps

Step 1 Click **Status and Statistics > Diagnostics > Copper Test**.

Step 2 Select the unit and port on which to run the test.

Step 3 Click **Copper Test**.

Step 4 When the message appears, click OK to confirm that the link can go down or Cancel to abort the test. The following fields are displayed in the Test Results block:

- Last Update—Time of the last test conducted on the port
- Test Results—Cable test results. Possible values are:
  - OK—Cable passed the test.
  - No Cable—Cable is not connected to the port.
  - Open Cable—Cable is connected on only one side.
  - Short Cable—Short circuit has occurred in the cable.
  - Unknown Test Result—Error has occurred.
- Distance to Fault—Distance from the port to the location on the cable where the fault was discovered.
- Operational Port Status—Displays whether port is up or down.

The Advanced Information block (supported on some of the port types) contains thefollowing information, which is refreshed each time you enter the page:

- Cable Length—Provides an estimate for the length.
- Pair—Cable wire pair being tested.
- Status—Wire pair status. Red indicates fault and Green indicates status OK.
- Channel—Cable channel indicating whether the wires are straight or cross-over.
- Polarity—Indicates if automatic polarity detection and correction has been activated for the wire pair.
- Pair Skew—Difference in delay between wire pairs.

Optical Module Status

The Optical Module Status page displays the operating conditions reported by the SFP (Small Form-factor Pluggable) transceiver.

The following GE SFP (1000Mbps) transceivers are supported:

- MGBLH1: 1000BASE-LH SFP transceiver, for single-mode fiber, 1310 nm wavelength, supports up to 40 km.
- MGBLX1: 1000BASE-LX SFP transceiver, for single-mode fiber, 1310 nm wavelength, supports up to 10 km.
- MGBSX1:1000BASE-SX SFP transceiver, for multimode fiber, 850 nm wavelength, supports up to 550 m.
- MGBT1: 1000BASE-T SFP transceiver for category 5 copper wire, supports up to 100 m.
- GLC-SX-MMD - 1000BASE-SX short wavelength; with DOM
- GLC-LH-SMD - 1000BASE-LX/LH long-wavelength; with DOM
- GLC-BX-D - 1000BASE-BX10-D downstream bidirectional single fiber; with DOM
- GLC-BX-U - 1000BASE-BX10-U upstream bidirectional single fiber; with DOM
- GLC-TE - 1000BASE-T standard

The following XG SFP+ (10,000Mbps) transceivers are supported:

- Cisco SFP-10G-SR
- Cisco SFP-10G-LR
- Cisco SFP-10G-SR-S
- Cisco SFP-10G-LR-S

The following XG passive cables (Twinax/DAC) are supported:

- Cisco SFP-H10G-CU1M
- Cisco SFP-H10G-CU3M
- Cisco SFP-H10G-CU5M

To view the results of optical tests, click **Status and Statistics** > **Diagnostics** > **Optical Module Status**.

This page displays the following fields:

- Port—Port number on which the SFP is connected
- Description—Description of optical transceiver
- Serial Number—Serial number of optical transceiver
- PID—Product ID of the transceiver
- VID—Version ID of the transceiver
- Temperature—Temperature (Celsius) at which the SFP is operating
- Voltage—SFPs operating voltage
- Current—SFPs current consumption
- Output Power—Transmitted optical power
- Input Power—Received optical power
- Transmitter Fault—Remote SFP reports signal loss. Values are True, False, and No Signal (N/S)
- Loss of Signal—Local SFP reports signal loss. Values are True and False
- Data Ready—SFP is operational. Values are True and False

Tech-Support Information

This page provides a detailed log of the device status. This is valuable when the technical support are trying to help a user with a problem, since it gives the output of many show commands (including debug command) in a single command.

To view technical support information useful for debugging purposes:

Step 1 Click **Status and Statistics** > **Diagnostics** > **Tech-Support Information**.

Step 2 Click **Generate**.

Note Generation of output from this command may take some time. When the information is generated, you can copy it from the text box in the screen by clicking on **Select tech-support data**.

RMON

Remote Networking Monitoring (RMON) enables an SNMP agent in the device to proactively monitor traffic statistics over a given period and send traps to an SNMP manager. The local SNMP agent compares actual, real-time counters against predefined thresholds and generates alarms, without the need for polling by a central SNMP management platform. This is an effective mechanism for proactive management, provided that you have set the correct thresholds relative to your network's base line.

RMON decreases the traffic between the manager and the device since the SNMP manager does not have to poll the device frequently for information, and enables the manager to get timely status reports, since the device reports events as they occur.

With this feature, you can perform the following actions:

- View the current statistics (from the time that the counter values cleared). You can also collect the values of these counters over a period of time, and then view the table of collected data, where each collected set is a single line of the History tab.
- Define interesting changes in counter values, such as "reached a certain number of late collisions" (defines the alarm), and then specify what action to perform when this event occurs (log, trap, or log and trap).

Statistics

The Statistics page displays detailed information regarding packet sizes and information regarding physical layer errors. The information is displayed according to the RMON standard. An oversized packet is defined as an Ethernet frame with the following criteria:

- Packet length is greater than MRU byte size.
- Collision event has not been detected.
- Late collision event has not been detected.
- Received (Rx) error event has not been detected.
- Packet has a valid CRC.

To view RMON statistics and/or set the refresh rate, complete the following:

Step 1 Click **Status and Statistics** > **RMON** > **Statistics**.

Step 2 Select the Interface for which Ethernet statistics are to be displayed.

Step 3 Select the Refresh Rate, which is the time period that passes before the interface statistics are refreshed.

The following statistics are displayed for the selected interface.

Bytes Received	Octets received, including bad packets and FCS octets, but excluding framing bits.
Drop Events	Packets dropped.
Packets Received	Good packets received including Multicast and Broadcast packets.
Broadcast Packets Received	Good Broadcast packets received. This number does not include Multicast packets.
Multicast Packets Received	Good Multicast packets received.
CRC & Align Errors	CRC and Align errors that have occurred.
Undersize Packets	Undersized packets (less than 64 octets) received.
Oversize Packets	Oversized packets (over 2000 octets) received.

Fragments	Fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.
Jabbers	Received packets that are longer than 1632 octets. This number excludes frame bits, but includes FCS octets that had either a bad FCS (Frame Check Sequence) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. A Jabber packet is defined as an Ethernet frame that satisfies the following criteria:
Collisions	Collisions received. If Jumbo frames are enabled, the threshold of Jabber frames is raised to the maximum size of Jumbo frames.
Frames of 64 Bytes	Frames, containing 64 bytes that were sent or received.
Frames of 65 to 127 Bytes	Frames, containing 65-127 bytes that were sent or received.
Frames of 128 to 255 Bytes	Frames, containing 128-255 bytes that were sent or received.
Frames of 256 to 511 Bytes	Frames, containing 256-511 bytes that were sent or received.
Frames of 512 to 1023 Bytes	Frames, containing 512-1023 bytes that were sent or received.
Frames of 1024 Bytes or More	Frames, containing 1024-2000 bytes, and Jumbo Frames, that were sent or received.

Note If one of the fields above shows a number of errors (not 0), a Last Update time is displayed.

Step 4 To view counters in table view or graphic view:

- Click **View All Interfaces Statistics** to see all ports in table view.
- Click **Graphic View** to display these results in graphic form. In this view, you can select the Time Span for which the results will be displayed and the type of statistic to be displayed.

History

The RMON feature enables monitoring statistics per interface.

The History page defines the sampling frequency, amount of samples to store and the port from which to gather the data. After the data is sampled and stored, it appears in the History Table page that can be viewed by clicking History Table.

To enter RMON control information, complete the following:

Step 1 Click **Status and Statistics** > **RMON** > **History**. The fields displayed on this page are defined in the Add RMON History page, below. The only field is that is on this page and not defined in the Add page is:

- Current Number of Samples-RMON is allowed by the standard not to grant all requested samples, but rather to limit the number of samples per request. Therefore, this field represents the sample number granted to the request that is equal or less than the requested value.

Step 2 Click **Add**.

Step 3 Enter the parameters.

- New History Entry-Displays the number of the new History table entry.
- Source Interface-Select the type of interface from which the history samples are to be taken.
- Max No. of Samples to Keep-Enter the number of samples to store.
- Sampling Interval-Enter the time in seconds that samples are collected from the ports. The field range is 1-3600.
- Owner-Enter the RMON station or user that requested the RMON information.

Step 4 Click **Apply**. The entry is added to the History Control Table page, and the Running Configuration file is updated.

Step 5 Click **History Table** to view the actual statistics.

Events

You can control the occurrences that trigger an alarm and the type of notification that occurs. This is performed as follows:

- Events Page—Configures what happens when an alarm is triggered. This can be any combination of logs and traps.
- Alarms Page—Configures the occurrences that trigger an alarm.

To define RMON events, complete the following steps:

Step 1 Click **Status and Statistics** > **RMON** > **Events**.

Step 2 Click **Add.**

Step 3 Enter the parameters.

- Event Entry—Displays the event entry index number for the new entry.
- Community—Enter the SNMP community string to be included when traps are sent (optional).
- Description—Enter a name for the event. This name is used in the Add RMON Alarm page to attach an alarm to an event.
- Notification Type—Select the type of action that results from this event. Values are:
  - None—No action occurs when the alarm goes off.
  - Log (Event Log Table)—Add a log entry to the Event Log table when the alarm is triggered.
  - Trap (SNMP Manager and Syslog Server)—Send a trap to the remote log server when the alarm goes off.
  - Log and Trap—Add a log entry to the Event Log table and send a trap to the remote log server when the alarm goes off.
- Owner—Enter the device or user that defined the event.

Step 4 Click **Apply**. The RMON event is saved to the Running Configuration file.

Step 5 Click **Event Log Table** to display the log of alarms that have occurred and that have been logged (see description below).

Alarms

RMON alarms provide a mechanism for setting thresholds and sampling intervals to generate exception events on counters or any other SNMP object counter maintained by the agent. Both the rising and falling thresholds must be configured in the alarm. After a rising threshold is crossed, no rising events are generated until the companion falling threshold is crossed. After a falling alarm is issued, the next alarm is issued when a rising threshold is crossed.

One or more alarms are bound to an event, which indicates the action to be taken when the alarm occurs.

Alarm counters can be monitored by either absolute values or changes (delta) in the counter values.

To enter RMON alarms, complete the following steps:

Step 1 Click **Status and Statistics** > **RMON** > **Alarms**.

All previously defined alarms are displayed. The fields are described in the Add RMON Alarm page below. In addition to those fields, the following field appears:

- Counter Value—Displays the value of the statistic during the last sampling period.

Step 2 Click **Add.**

Step 3 Enter the parameters.

Alarm Entry	Displays the alarm entry number.
Interface	Select the type of interface for which RMON statistics are displayed.
Counter Name	Select the MIB variable that indicates the type of occurrence measured.
Sample Type	Select the sampling method to generate an alarm. The options are: • Absolute—If the threshold is crossed, an alarm is generated. • Delta—Subtracts the last sampled value from the current value The difference in the values is compared to the threshold. If the threshold was crossed, an alarm is generated.
Rising Threshold	Enter the value that triggers the rising threshold alarm.
Rising Event	Select an event to be performed when a rising event is triggered. Events are configured in the Events, on page 19.
Falling Threshold	Enter the value that triggers the falling threshold alarm.
Falling Event	Select an event to be performed when a falling event is triggered.

Startup Alarm	Select the first event from which to start generation of alarms. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold. • Rising Alarm—A rising value triggers the rising threshold alarm. • Falling Alarm—A falling value triggers the falling threshold alarm. • Rising and Falling—Both rising and falling values trigger the alarm.
Interval	Enter the alarm interval time in seconds.
Owner	Enter the name of the user or network management system that receives the alarm.

Step 4 Click **Apply**. The RMON alarm is saved to the Running Configuration file.

sFlow

The sFlow monitoring system consists of an sFlow agent (embedded in a switch or router or in a stand alone probe) and a central data collector, known as the sFlow collector. The sFlow agent uses sampling technology to capture traffic and statistics from the device it is monitoring. sFlow datagrams are used to forward the sampled traffic and statistics to an sFlow collector for analysis.

sFlow V5 defines:

- How traffic is monitored.
- The sFlow MIB that controls the sFlow agent.
- The format of the sample data used by the sFlow agent when forwarding data to a central data collector. The device provides support for two types of sFlow sampling: flow sampling and counters sampling. The following counters sampling is performed according to sFlow V5 (if supported by the interface):
  - Generic interface counters (RFC 2233)
  - Ethernet interface counters (RFC 2358)

sFlow Receivers

The sFlow receiver defines the set of objects used to maintain a sFlow session between a sFlow Agent and a sFlow Collector. To set the sFlow receiver parameters, follow these steps:

Step 1 Click **Status and Statistics**>**sFlow** >**sFlow Receivers**.

Step 2 Enter the following fields:

- IPv4 Source Interface—Select the IPv4 source interface.

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

- IPv6 Source Interface— Select the IPv6 source interface

Step 3 To add a receiver (sFlow analyzer), click **Add** and select one of the pre-defined sampling definition indices in Receiver Index.

Step 4 Enter the receiver's address fields:

- Receiver Definition—Select whether to specify the sFlow server By IP address or By name.

  If Receiver Definition is By IP Address:

- IP Version—Select whether an IPv4 or an IPv6 address for the server is used.
- IPv6 Address Type—Select the IPv6 address type (if IPv6 is used). The options are:
  - Link Local —The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- Link Local Interface—Select the link local interface (if IPv6 is used) from the list.

Step 5 Enter the following fields:

- Receiver IP Address/Name—Enter the IP address or the name of the receiver, whichever is relevant.
- Port—Port to which SYSLOG messages are sent.
- Maximum Datagram Size—Maximum number of bytes that can be sent to the receiver in a single sample datagram (frame).

Step 6 Click **Apply**.

sFlow Interface Settings

To sample datagrams or counters from a port, the port must be associated with a receiver. sFlow port settings can be configured only after a receiver has been defined in the sFlow Receivers, on page 21 pages.

To enable sampling and configure the port from which to collect the sFlow information, follow these steps:

Step 1 Click **Status and Statistics** > **sFlow** > **sFlow Interface Settings**.

The sFlow interface settings are displayed.

Step 2 To associate an sFlow receiver with a port, select a port, click **Edit**, and enter the fields:

- Interface—Select the unit/port from which information is collected.
- (Flow Sampling) State—Enable/disable flow sampling.
- Sampling Rate—If x is entered, a flow sample will be taken for each x frame.
- Maximum Header Size—Maximum number of bytes that should be copied from a sampled packet.
- Receiver Index—Select one of the indices that was defined in the sFlow Receivers, on page 21 pages.

- (Counter Sampling) State—Enable/disable counters sampling.
- Sampling Interval—If x is entered, this specifies that a counter sample will be taken for each x seconds.
- Receiver Index—Select one of the indices that was defined in these sFlow Receivers, on page 21 pages.

Step 3 Click **Apply**.

sFlow Statistics

To view the sFlow statistics, complete the following:

Step 1 Click **Status and Statistics > sFlow > sFlow Statistics**.

Step 2 Select the Refresh Rate from the drop-down menu. (No Refresh, 15 sec, 30 sec or 60 sec)

Step 3 Next, in the sFlow Statistics Table, filter the interface type by using the drop-down menu and click **Go**

The following info will be displayed:

- Port—Port for which sample was collected.
- Packets Sampled—Number of packets sampled.
- Datagrams Sent to Receiver—Number of sFlow sampling packets sent.

Step 4 Click on one of the following to clear the interfaces counter(s) or refresh the counter.

- Clear Interface Counters—Clears interface counters.
- Clear All Interface Counters—Clears all interface counters.
- Refresh—Refreshes the counters.

View Log

The device can write to the following logs:

- Log in RAM (cleared during reboot).
- Log in Flash memory (cleared only upon user command).

You can configure the messages that are written to each log by severity, and a message can go to more than one log, including logs that reside on external SYSLOG servers.

RAM Memory

The RAM Memory page displays all messages that are saved in the RAM (cache) in chronological order. All entries are stored in the RAM log.

Pop-Up SYSLOG Notifications

When a new SYSLOG message is written to the RAM log file, a notification is displayed on the web GUI showing its contents. The web GUI polls the RAM log every 10 seconds. Syslog notifications pop-ups for all SYSLOGs created in the last 10 seconds appear at the bottom right of the screen.

If more than 7 pop-up notifications are displayed, a summary pop-up is displayed. This pop-up states how many SYSLOG notifications aren't displayed. It also contains a button that enables closing all of the displayed pop-ups.

To view log entries, click **Status and Statistics** > **View Log** > **RAM Memory**.

The following are displayed at the top of the page:

- Alert Icon Blinking—Toggles between disable and enable.
- Pop-Up Syslog Notifications—Enables receiving pop-up SYSLOGs as described above.
- Current Logging Threshold—Specifies the levels of logging that are generated. This can be changed by clicking Edit by the field's name.

This page contains the following fields for every log file:

- Log Time—Time when message was generated.
- Severity—Event severity
- Description—Message text describing the event

To clear the log messages, click **Clear Logs.**

Flash Memory

The Flash Memory page displays the messages that stored in the Flash memory, in chronological order. The minimum severity for logging is configured in the Log Settings. Flash logs remain when the device is rebooted. You can clear the logs manually.

To view the Flash logs, click **Status and Statistics** > **View Log** > **Flash Memory**.

The Current Logging Threshold specifies the levels of logging that are generated. This can be changed by clicking Edit by the field's name.

This page contains the following fields for each log file:

- Log Index—Log entry number
- Log Time—Time when message was generated.
- Severity—Event severity
- Description—Message text describing the event

To clear the messages, click **Clear Logs.** The messages are cleared.