

Status and Statistics

This chapter contains the following sections:

- System Summary, on page 1
- CPU Utilization, on page 3
- Port Utilization, on page 3
- Interface, on page 4
- Etherlike, on page 5
- GVRP, on page 6
- 802.1X EAP, on page 7
- ACL, on page 8
- Hardware Resource Utilization, on page 9
- Health and Power, on page 9
- SPAN , on page 10
- Diagnostics, on page 11
- Onboard Packet Capture , on page 15
- RMON, on page 18
- View Log, on page 24

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. To edit the settings below, click **Edit** to go System Settings to enter this value.

- System Description—A description of the system.
- System Location—Physical location of the device.
- System Contact—Name of a contact person.

- Host Name—Name of the device. 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.
- 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

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

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

TCP/UDP Services Status

To reset the following fields, click **Edit**. The following settings will be displayed.

- 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 link you directly to the Properties. This page shows 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 1 (Active)—Device model ID.
- Serial Number—Serial number.
- PID VID—Part number and version ID.

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:

Procedure

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 the utilization of the broadband (both incoming and outgoing) per port.

To display the port utilization, follow these steps:

Procedure

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

Step 2 Select 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:

- TX Utilization—Check to display TX utilization data.
- RX Utilization—Check to display RX utilization data.
- 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:

Procedure

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 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:

Procedure

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- Number of pause 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 Generic Attribute Registration Protocol (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's 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:

Procedure

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

Step 2 Configure 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.

Received - Transmitted

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.

GVRP Error Statistics

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 the interface counters, click **Clear All Interface Counters.**

Step 4 To refresh the data, click **Refresh**.

Step 5 To view all interface statistics, click **View 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:

Procedure

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.

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 Click **Clear Interface Counters** to clear the counters of all interfaces.

Step 5 Click **Refresh** to refresh the counters.

Step 6 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:

Procedure

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 in the Hardware Resources Table:

- 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.
- 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. To access the Health and Power page, navigate to **Status and Statistics > Health and Power.**

The following sections will be displayed.

Environment Status

- Fan Status—Displays whether the fan is not available (N/A) or is available and is operating normally (OK) or not (Failure).
- 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 available.

Power Supply Status

Main Power Supply Status—Displays 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.

SPAN

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.

SPAN 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's the analyzer port.

To add a destination port, follow these steps:

Procedure

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

Step 2 In the Session Destinations Table, click **Add**.

Step 3 Enter the following fields:

- Session ID—Select a session ID. This must match the session IDs of the source ports.
- Port—Select the port from the drop-down list.
- Network Traffic—Select to enable that traffic other than monitored traffic is possible on the port.

Step 4 Click **Apply**.

SPAN 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 only SPAN support - 4 sessions and up to 8 source interfaces in each. The interfaces in LAG can be defined as source interfaces. If exceeded, it will generate errors.

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

Procedure

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

Step 2 In the SPAN Source Table click **Add**.

Step 3 Select the 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's set to the Down state and communications are interrupted. After the test, the port returns to the Up state. It's not recommended that you run the copper port test on a port you're 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.:

Procedure

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

Step 2 Select the 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 isn't 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 the port is up or down.

The Advanced Information block (supported on some of the port types) contains the following 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 have 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:

- CWDM-SFP-1490
- CWDM-SFP-1510
- CWDM-SFP-1550
- CWDM-SFP-1570
- CWDM-SFP-1590
- 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:

- SFP-10G-ER
- SFP-10G-ER-S
- SFP-10G-BXD-I
- SFP-10G-BXU-I
- Cisco SFP-10GBase-T
- 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:

- SFP-H10GB-CU1-5M
- SFP-H10GB-CU2M
- SFP-H10GB-CU2-5M
- SFP-H10GB-ACU10M
- SFP-10G-AOC1M
- SFP-10G-AOC3M
- SFP-10G-AOC5M
- SFP-10G-AOC7M
- SFP-10G-AOC10M
- 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 technical support is trying to help you with a problem, since it gives the output of many show commands (including a debug command) in a single command.

To view technical support information useful for debugging purposes:

Procedure

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** and then copying and pasting the text into another document.

Onboard Packet Capture



Note Onboard packet capture support was added in release 4.1.3x and is supported on all Catalyst 1200 and 1300 switches.

The Onboard Packet Capture (OBC) enhances troubleshooting capabilities on the device. It provides the ability to capture packets that are received and sent by the switch CPU (known because the control plane). The packet captures can then be saved to local storage, and then exported for offline analysis. The entity used to define the capture parameters and to activate the captures is called a capture point. The device supports up to 4 capture points and 20 Mega Byte because buffer for the captured packets.

To export the capture buffer to a file on the local flash or on the USB go to the Buffer File Operation.

1. Crash Capture Destination is a setting that is used to export a capture file if the device crashes. In this scenario, the user will not be able to export the file manually. Therefore, the export destination must be defined manually. Select the destination device for saving the file:
   - Flash – do save the file to the device flash.
   - USB – to save the device to a USB storage device connected to the device.



Note In this case the name of the capture file is set automatically and will indicate the date and time of capture.

Capture Point Settings

Note This setting is only available in Advanced Mode.

To define and activate a capture point, perform the following steps.

Procedure

Step 1 Navigate to **Status and Statistics > Onboard Packet Capture > Capture Point Settings.**

Step 2 Click **Add** to add a capture point and configure the following:

- Capture Point Name –The name of the capture point.
- Buffer Mode – Define the capture mode to one of the following:
  - Linear – capture will be terminated when the capture buffer is full.
  - Circular – the capture wraps up when the buffer is full and rewrite the packets in the beginning of the buffer.
- Buffer Size (MB): Define the size of the capture buffer in MB. The buffers for all capture points cannot exceed 20MB.
- Interface – only the Control Plane (CPU) interface is supported.
- Capture Direction: define the direction of the traffic to capture: both inbound and outband traffic (both), only inbound traffic (in) or only outband traffic (out).

Step 3 Click **Apply**.

Step 4 To edit or delete a capture point, select the capture point and click **Edit** or **Delete**.

Step 5 To activate a capture point, select one of the capture points from the table and click **Operations**. In the Capture Point Operation field select **Activate** and click **Apply**. The state of the capture point in the Capture Point Settings Table is set to **Active**.

Step 6 To deactivate an active capture point, select an active capture point and click **Operations**. In the Capture Point Operation field, select **Deactivate** and click **Apply**. The state of the capture point in the Capture Point Settings Table is set to **Inactive**.

Buffer File Operation

Note This setting is only available in Advanced Mode.

The captured packets are stored in a memory buffer. To copy the packets to a nonvolatile memory for further debugging perform the following steps:

Procedure

Step 1 Navigate to **Status and Statistics > Onboard Packet Capture > Buffer File Operation**.

Step 2 If the device crashes during a capture, the packets are saved automatically to a nonvolatile memory. Select the destination device for saving the crash report.

- Flash – do save the file to the device flash. (Default)
- USB – to save the device to a USB storage device connected to the device.

Step 3 Click **Apply to** save the configuration for the **Crash Capture Destination**.

Step 4 To manually export one of the capture point buffers, navigate to the **Export Capture** section of the screen and configure the following:

- Capture Point Name – Select the capture point that you want to export.
- Capture File Name – Define a name for the exported file.
- Export Destination – Select the destination device for saving the file:
  - Flash – do save the file to the device flash.
  - USB – to save the device to a USB storage device connected to the device.

The file can be exported in Flash or USB based on the selection.

Step 5 To export the Capture Point file, click **Export.**

Buffer Statistics

Note This setting is available only in Advanced Mode.

To view the capture buffer statistics, complete the following steps:

Procedure

Step 1 Navigate to **Status and Statistics > Onboard Packet Capture > Buffer Statistics.**

Step 2 In the **Capture Point Name** field, select the capture buffer from the drop-down list to view the statistics.

Step 3 Next, select the Refresh Rate from the following options:

- No Refresh
- 15 sec
- 30 sec

- 60 sec

Step 4 The following statistics will be displayed:

- Buffer State – Active or Inactive
- Buffer Mode – Linear or circular
- Buffer Size (KB) – The size of the buffer in Kilobytes
- Captured Packets – The number of the packets capture
- Buffer Used (KB) – The actual buffer size that is used.
- Packet Capture Rate per Second – The packet per second rate of the traffic that was captured.
- Packets Dropped – The number of packets that were dropped during the capture session.

Step 5 To manually refresh the information click **Refresh**.

Step 6 To clear the buffer – click **Clear Buffer**.

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.
- A collision event hasn't been detected.

- A late collision event hasn't been detected.
- Received (Rx) error event hasn't been detected.
- The packet has a valid CRC.

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

Procedure

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

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

Step 3 Select the Refreshed 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 doesn't include Multicast packets.
Multicast Packets Received	Good Multicast packets received.
CRC & Align Errors	CRC and Align errors that have occurred.
Undersize Packets	Undersized packets (fewer 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 nonintegral 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 65–127 Bytes	Frames, containing 65-127 bytes that were sent or received.
Frames of 128–255 Bytes	Frames, containing 128-255 bytes that were sent or received.

Frames of 256–511 Bytes	Frames, containing 256-511 bytes that were sent or received.
Frames of 512–1023 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 preceding fields shows some errors (not 0), a Last Update time is displayed.

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

- Click **Clear Interface Counters** to clear the data.
- Click **Refresh** to refresh the data.
- 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 and frame size for which the results will 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:

Procedure

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.

Step 6 Click **History Control Table** to view the History Control Table.

Step 7 From the History Entry No. drop down menu, optionally select the entry number of the sample to display.

The fields are displayed for the selected sample.

- Owner-History table entry owner.
- Sample No.-Statistics taken from this sample.
- Drop Events-Dropped packets due to lack of network resources during the sampling interval. This may not represent the exact number of dropped packets, but rather the number of times dropped packets detected.
- Bytes Received-Octets received including bad packets and FCS octets, but excluding framing bits.
- Packets Received-Packets received, including bad packets, Multicast, and Broadcast packets.
- Broadcast Packets-Good Broadcast packets excluding Multicast packets.
- Multicast Packets-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) received, excluding framing bits, but including FCS octets.
- Jabbers-Total number of received packets that longer than 2000 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.
- Collisions-Collisions received.
- Utilization-Percentage of current interface traffic compared to maximum traffic that the interface can handle.

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:

Procedure

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.

The following data will be displayed:

- Event Entry No.—Event entry number
- Log No.—Event log number
- Log Time—Time of event log
- Description—Description of event log.

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:

Procedure

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 21.
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.

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.

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 Index—Log ID
- Log Time—Time when a 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 are 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.

The Flash Memory Log Table contains the following fields for each log file:

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

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