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**.

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.
  - Select the refresh rate from the Refresh Rate drop-down menu.

- Select an interface and click **Clear Interface Counters** to clear the statistics counters for the selected interface.
- Click **Clear All Interface Counters** to clear the statistics counters for all interfaces.
- Select an interface and click **View Interface Statistics** to see the statistics counters for the selected interface on a single page.
- Click **Refresh** to manually refresh the statistics counters for all interfaces.

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 To view statistics counters in table view, click **View All Interfaces Statistics** to see all ports in table view.

- Select the refresh rate from the Refresh Rate drop-down menu.
- Select an interface and click **Clear Interface Counters** to clear the statistics counters for the selected interface.

- Click **Clear All Interface Counters** to clear the statistics counters for all interfaces.
- Select an interface and click **View Interface Statistics** to see the statistics counters for the selected interface on a single page.
- Click **Refresh** to manually refresh the statistics counters for all interfaces.

Step 3 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 - Received flow control pause frames.
- Pause Frames Transmitted - Number of flow control pause frames transmitted from the selected interface.

Step 4 You can also click **Refresh** to refresh the stats or click **Clear Interface Counters** to clear 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.

The count of each item may differ from different Models due to system design. Also, because of ASIC characteristics, it’s possible to show a "Lack of HW resources" when binding an Advance QoS service policy or User-defined ACL but this page shows enough TCAM resources.

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

The following fields are displayed:

- Total Entries
  - Maximum—Number of available TCAM entries that can be used for whole system.
  - In Use—Number of TCAM entries used for whole system
- System Rules
  - Allocated—Number of allocated TCAM entries that can be used for system rules.

- In Use—Number of TCAM entries used for system rules.

- ACL and QoS Rules
  - Allocated—Number of allocated TCAM entries that can be used for ACL and QoS rules.
  - In Use—Number of TCAM entries used for ACL and QoS rules.

Health

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

Fan Status

- Fan—Displays fan ID.
- Status—Displays whether the fan is operating normally (OK) or not (Fault).
- Speed (RPM)—Displays fan speed.

Temperature Status

- Sensor—Displays sensor id.
- Status—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.
- TEMP (°C) —Displays temperature of sensor.

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, multipledevice 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.

RSPAN supports source ports, source VLANs, and destination ports on different switches, enabling remote monitoring of multiple switches across your network. 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

RSPAN traffic from the source ports or VLANs is copied into the RSPAN VLAN and forwarded carrying the RSPAN VLAN to a destination session monitoring the RSPAN VLAN.

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.

RSPAN VLAN

An RSPAN VLAN carries SPAN traffic between RSPAN source and destination sessions.

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

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

Step 2 Select the RSPAN VLAN.

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 a local interface or remote VLAN as destination.
- Port—Select a 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**.

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.

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

Step 1 Click **Status and Statistics** > **SPAN and 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 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 5 Click **Apply**. The source interface for the mirroring is configured.

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).

RMON 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.

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

Step 4 To view counters in table view:

- Click **View All Interfaces Statistics** to see all ports in table view.

RMON 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.

RMON Events

The Events page displays the log of events (actions) that occurred. Two types of events can be logged: Log or Log and Trap. The action in the event is performed when the event is bound to an alarm and the conditions of the alarm have occurred.

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—Entera 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 goesoff.
  - Log (Event Log Table)—Add a log entry to the Event Log table when the alarm istriggered.
  - 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.

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.
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.

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.

- 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 entry number
- 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.