Configuration — System Monitoring
Avaya Ethernet Routing Switch 2500 Series

Release 4.3
NN47215-502, 04.02
November 2010
Notice
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Download documents
For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support
## Contents

### Chapter 1: New in this release
- Features.........................................................................................................................7
  - EDM MIB Web page........................................................................................................7
  - EDM Trap Web page.....................................................................................................7
- Other changes..................................................................................................................7
  - Enterprise Device Manager.........................................................................................8

### Chapter 2: Introduction
- ACLI command modes..................................................................................................9

### Chapter 3: System Monitoring Fundamentals
- Navigation......................................................................................................................11
- CPU and memory utilization.........................................................................................11
- Light Emitting Diode display.......................................................................................12
- EDM MIB Web page......................................................................................................12
- SNMP traps..................................................................................................................12
- System Log...................................................................................................................12
- Port mirroring...............................................................................................................13
  - Port mirroring configuration rules...........................................................................13
- Stack monitor...............................................................................................................14
- Chassis and port statistics...........................................................................................14
- Remote Monitoring......................................................................................................15
- RMON alarms.............................................................................................................15

### Chapter 4: Network monitoring configuration using ACLI
- Navigation......................................................................................................................19
- CPU utilization.............................................................................................................19
- Memory utilization.......................................................................................................20
- System log....................................................................................................................20
  - Viewing the system event log..................................................................................21
  - Configuring system logging.....................................................................................21
  - Disabling logging.......................................................................................................22
  - Setting default logging.............................................................................................22
  - Clearing log messages...............................................................................................23
- Port mirroring...............................................................................................................23
  - Displaying the port-mirroring configuration............................................................24
  - Configuring port-mirroring.......................................................................................24
  - Disabling port-mirroring...........................................................................................25
- Port statistics...............................................................................................................25
  - Displaying port-statistics...........................................................................................25
  - Clearing statistical information.................................................................................26
- Stack health..................................................................................................................27
  - Viewing stack health................................................................................................27
  - Viewing stack monitor information........................................................................28
  - Configuring the stack monitor................................................................................28
  - Disabling the stack monitor.....................................................................................29

### Chapter 5: Network monitoring configuration using Enterprise Device Manager
- Navigation......................................................................................................................31
Chapter 6: RMON using ACLI.................................................................................................59
  Viewing the RMON alarms.................................................................................................59
  Viewing the RMON events.................................................................................................60
  Viewing the RMON history.................................................................................................60
  Viewing the RMON statistics.............................................................................................60
  Viewing RMON history for a port......................................................................................61
  Viewing RMON packets for a port......................................................................................61
  Viewing RMON statistics for a port....................................................................................62
  Configuring RMON alarms.................................................................................................62
  Deleting RMON alarms.......................................................................................................63
  Configuring RMON events settings..................................................................................64
  Deleting RMON events settings.......................................................................................64
  Configuring RMON history settings................................................................................65
  Deleting RMON history settings......................................................................................65
  Configuring RMON statistics settings.............................................................................66
  Deleting RMON statistics.................................................................................................66

Chapter 7: RMON using Enterprise Device Manager.........................................................69
  Navigation.........................................................................................................................69
  Working with RMON information....................................................................................69
    Viewing statistics.............................................................................................................70
    Viewing RMON history..................................................................................................72
    Creating RMON history characteristics.........................................................................73
    Disabling RMON history...............................................................................................74
    Graphing RMON history statistics...............................................................................74
    Enabling Ethernet statistics gathering............................................................................76
Disabling Ethernet statistics gathering................................................................................................... 76
Creating an alarm............................................................................................................................................77
Deleting an alarm............................................................................................................................................78
Using RMON events....................................................................................................................................... 79
  Viewing an event.................................................................................................................................... 79
  Creating an event................................................................................................................................... 80
  Deleting an event....................................................................................................................................81
Viewing RMON log information....................................................................................................................... 81
Chapter 1: New in this release

The following sections detail what’s new in Configuration — System Monitoring (NN47215-502) for Release 4.3

- **Features** on page 7
- **Other changes** on page 7

---

**Features**

See the following sections for information about feature changes:

- **EDM MIB Web page** on page 7
- **EDM Trap Web page** on page 7

---

**EDM MIB Web page**

You can use Enterprise Device Manager (EDM) MIB Web page to query SNMP objects on the switch. For more information, see

- **EDM MIB Web page** on page 12
- **Using the EDM MIB Web page for SNMP Get and Get-Next** on page 57
- **Using the EDM MIB Web page for SNMP walk** on page 57

---

**EDM Trap Web page**

You can use the EDM Trap Web page to enable or disable traps received by the SNMP trap receiver. For more information, see the following:

  **SNMP traps** on page 12

---

**Other changes**

See the following sections for information about changes that are not feature-related:
Enterprise Device Manager

Enterprise Device Manager (EDM) replaces both the Java-based Device Manager and Web-based management user interfaces. EDM is an embedded element management and configuration application for Ethernet Routing Switch 2500 Series switches. EDM provides a Web-based graphical user interface through a standard web browser for the convenience of full configuration and management on the switch, and retains the look and feel of Device Manager.

Multiple Port Configuration

Among the many functions available in EDM, you can configure port-specific features for a single port, a group of ports, or all ports. Multiple Port Configuration appears as a pane in the work area wherever this function is available. By default the pane appears and you can close and open it with a click of the task bar.

For more information about EDM, see Ethernet Routing Switch 2500 Series Fundamentals, (NN47215-102).
Chapter 2: Introduction

This guide provides information about system logging, displaying system statistics, and configuring network monitoring on the Avaya Ethernet Routing Switch 2500 Series. This guide describes the features of the following Avaya switches.

- Avaya Ethernet Routing Switch 2526T
- Avaya Ethernet Routing Switch 2526T-PWR
- Avaya Ethernet Routing Switch 2550T
- Avaya Ethernet Routing Switch 2550T-PWR

The term "Ethernet Routing Switch 2500 Series" is used in this document to describe the features common to the switches mentioned in the preceding list.

A switch is referred to by its specific name while describing a feature exclusive to the switch.

### ACLI command modes

ACLI provides the following command modes:

- User EXEC
- Privileged EXEC
- Global Configuration
- Interface Configuration

Mode access is determined by access permission levels and password protection.

If no password is set, you can enter ACLI in User EXEC mode and use the `enable` command to move to the next level (Privileged EXEC mode). However, if you have read-only access, you cannot progress beyond User EXEC mode, the default mode. If you have read-write access you can progress from the default mode through all of the available modes.

With sufficient permission, you can use the rules in the following table to move between the command modes.

#### Table 1: ACLI command modes

<table>
<thead>
<tr>
<th>Command mode and sample prompt</th>
<th>Entrance commands</th>
<th>Exit commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC 2526T&gt;</td>
<td>No entrance command, default mode</td>
<td>exit</td>
</tr>
<tr>
<td>Command mode and sample prompt</td>
<td>Entrance commands</td>
<td>Exit commands</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Privileged EXEC 2526T#</td>
<td>enable</td>
<td>exit or logout</td>
</tr>
<tr>
<td>Global Configuration 2526T(config)#</td>
<td>From Privileged EXEC mode, enter: configure</td>
<td>To return to Privileged EXEC mode, enter: end or exit To exit ACLI completely, enter: logout</td>
</tr>
<tr>
<td>Interface Configuration 2526T(config-if)#</td>
<td>From Global Configuration mode: To configure a port, enter: interface fastethernet &lt;port number&gt; To configure a VLAN, enter: interface vlan &lt;vlan number&gt;</td>
<td>To return to Global Configuration mode, enter: exit To return to Privileged EXEC mode, enter: end To exit ACLI completely, enter: logout</td>
</tr>
</tbody>
</table>

For more information about ACLI, see *Avaya Ethernet Routing Switch 2500 Series Fundamentals*, (NN47215-102).
The Avaya Ethernet Routing Switch 2500 Series provide features that allow you to monitor your network, display switch statistics, log system events, and provide Remote Network Monitoring (RMON). This chapter contains information about the following topics:

**Navigation**

- CPU and memory utilization on page 11
- Light Emitting Diode display on page 12
- EDM MIB Web page on page 12
- SNMP traps on page 12
- System Log on page 12
- Port mirroring on page 13
- Stack monitor on page 14
- Chassis and port statistics on page 14
- Remote Monitoring on page 15

**CPU and memory utilization**

The CPU utilization feature provides data for CPU and memory utilization. You can view CPU utilization information for the past 10 seconds (s), 1 minute (min), 1 hour (hr), 24 hr, or since system startup. The switch displays CPU utilization as a percentage. With CPU utilization information you can see how the CPU was used during a specific time interval.

The memory utilization provides information about the percentage of the dynamic memory currently used by the system. The switch displays memory utilization in terms of the lowest percentage of dynamic memory available since system startup.

No configuration is required for this display-only feature.
Light Emitting Diode display

The Avaya Ethernet Routing Switch 2500 Series displays diagnostic and operation information though the LEDs on the unit. Familiarize yourself with the interpretation of the LEDs on the 2500 series device. For more information about the interpretation of the LEDs, see Avaya Ethernet Routing Switch 2500 Series — Installation (NN47205-300).

EDM MIB Web page

You can use the EDM MIB Web page to view the response of an SNMP Get and Get-Next request for an Object Identifier (OID) or object name.

With the SNMP walk, you can retrieve a subtree of the Management Information Base (MIB) that has the object as root by using Get-Next requests.

The MIB Web page does not support the following features:

• displaying SNMP SET requests
• displaying SNMP tables
• translating MIB enumerations (that is, displaying the name [interpretation] of number values of objects defined as enumerations in the MIB)

SNMP traps

Simple Network Management Protocol (SNMP) traps are configured as notification controls. For more information about notification controls, see Avaya Ethernet Routing Switch 2500 Series Configuration — Security, (NN47205-505).

System Log

The System Log displays messages obtained from system Non Volatile Random Access Memory (NVRAM) or Dynamic Random Access Memory (DRAM). The System Log displays only the data for the Avaya Ethernet Routing Switch 2500 Series through the Console or Comm port or Telnet.
System Log messages operate as follows:

- NVRAM messages are retrievable after a system reset.
- DRAM messages can be viewed while the system is operational.
- All NVRAM and DRAM messages are time stamped.
- When you restart your system after a reset, the DRAM messages are deleted.
- After a reset, all messages stored in NVRAM are copied to DRAM (DRAM messages are not copied to NVRAM). The messages copied to DRAM are time stamped to zero (0).

**Port mirroring**

With the Port mirroring feature, also referred to as conversation steering, you can allocate a single switch port (monitor port) as a traffic monitor for another switch port (mirror port). All incoming traffic on the mirrored port is copied to the monitor port. This operation excludes traffic forwarded by the switch. This feature is helpful in network troubleshooting.

You can specify port-based monitoring for ingress to a specific port. You can also attach a probe device or equivalent, to the designated monitor port. When a port is operating as a monitor port, forwarding is not allowed on that port.

Avaya Ethernet Routing Switch 2500 Series supports ingress, egress, and ingress/egress port-based mirroring.

**Port mirroring configuration rules**

The following configuration rules apply to the various port mirroring modes:

Port mirroring ingress mode (XRX or ->Port X)—In the Port mirroring ingress mode, packets received on mirror port X are copied to the monitor port.

Standalone—On a standalone switch there is no limitation for ingress port mirroring.

Stack—To enable ingress port mirroring in a stack environment, the mirror port and the monitor port can be on any unit in the stack.

Port mirroring egress mode (XTX or Port X ->)—In the Port mirroring egress mode, packets transmitted on mirror port X are copied to the monitor port.

Standalone—On a standalone switch, there is no limitation for ingress port mirroring.

Stack—To enable egress port mirroring in a stack environment, the mirror port and the monitor port can be on any unit in the stack.
Port mirroring ingress and egress mode (XRX or XTX or <->Port X)—In the Port Mirroring ingress and egress mode, packets that are either transmitted or received on mirror port X are copied to the monitor port.

Standalone—On a standalone switch, there is no limitation for ingress port mirroring.

Stack—Concurrent ingress and egress port mirroring is not supported in stack configurations.

---

Stack monitor

The Stack Monitor uses a set of control values to enable its operation, to set the expected stack size, and to control the frequency of trap sending. The stack monitor, if enabled, detects problems with the units in the stack and sends a trap.

The stack monitor sends a trap for the following events.

- The number of units in a stack changes.
- The trap sending timer expires.

Each time the number of units in a stack changes, the trap sending timer resets and the stack monitor compares the current number of stack units with the configured number of stack units. If the values are not equal, the switch sends a trap and logs a message to syslog. The stack monitor sends traps from a stand-alone unit or the base unit of the stack.

After the trap sending timer reaches the configured number of seconds at which traps are sent, the switch sends a trap and logs a message to syslog and restarts the trap sending timer. The syslog message is not repeated unless the stack configuration changes. To prevent the log from being filled with stack configuration messages.

After you enable the stack monitor on a stack, the stack monitor captures the current stack size and uses it as the expected stack size. You can choose a different value and set it after you enable the feature.

---

Chassis and port statistics

Chassis and port statistics allow you to view detailed information about any switch or port. The port statistics are divided by received and transmitted so that you can compare and evaluate throughput or other port parameters.
Remote Monitoring

Remote monitoring (RMON) MIB is an interface between the RMON agent on an Ethernet Routing Switch 2500 Series switch and an RMON management application, such as Enterprise Device Manager.

The RMON agent defines objects that are suitable for the management of any type of network, but some groups are targeted for Ethernet networks in particular.

The RMON agent continuously collects statistics and proactively monitors switch performance. You can view this data through ACLI and EDM.

RMON has three major functions:

• creating and displaying alarms for user-defined events
• gathering cumulative statistics for Ethernet interfaces
• tracking a history of statistics for Ethernet interfaces

RMON alarms

Alarms are useful when you need to know when the values of a variable go out of range. You can define an RMON alarm for any MIB variable that resolves to an integer value. You cannot use string variables (such as system description) as alarm variables.

All alarms share the following characteristics:

• An upper and lower threshold value is defined.
• A corresponding rising and falling event occurs.
• An alarm interval or polling period is reached.

When alarms are activated, you can view the activity in a log or a trap log, or you can create a script to notify you by sending an audible sound to a console, sending e-mail, or calling a pager.

How RMON alarms work

The alarm variable is polled and the result is compared against upper and lower limit values you select after you create the alarm. If either limit is reached or crossed during the polling period then the alarm triggers and generates an event that you can view in the event log or the trap log.

The upper limit of the alarm is called the rising value, and its lower limit is called the falling value. RMON periodically samples the data based upon the alarm interval. During the first interval in which the data passes above the rising value, the alarm triggers as a rising event.
During the first interval in which the data drops below the falling value, the alarm triggers as a falling event.

The following figure describes how alarms are triggered.

![Figure 1: RMON alarm triggers](image)

The alarm fires during the first interval that the sample goes out of range. No additional events are generated for that threshold until the opposite threshold is crossed. Therefore, it is important to carefully define the rising and falling threshold values for alarms to work as expected. Otherwise, incorrect thresholds cause an alarm to fire at every alarm interval.

A general guideline is to define one of the threshold values to an expected baseline value, and then define the opposite threshold as the out-of-bounds limit. Because of sample averaging, the value may be equal to ±1 of the baseline units. For example, assume an alarm is defined on octets going out of a port as the variable. The intent of the alarm is to provide notification to you after excessive traffic occurs on that port. If spanning tree is enabled, 52 octets are transmitted out of the port every 2 seconds, which is equivalent to baseline traffic of 260 octets every 10 seconds. This alarm provides notification to you if the lower limit of octets going out is defined at 260 and the upper limit is defined at 320 (or at a value greater than 260 + 52 = 312).

The first time outbound traffic other than spanning tree Bridge Protocol Data Units (BPDU) occurs, the rising alarm fires. After outbound traffic other than spanning tree ceases, the falling alarm fires. This process provides you with time intervals of a non-baseline outbound traffic.

If the alarm is defined with a falling threshold less than 260 (assuming the alarm polling interval is 10 seconds) the rising alarm can fire only once. For the rising alarm to fire a second time, the falling alarm (the opposite threshold) must fire. Unless the port becomes inactive or spanning tree is disabled (which causes the value for outbound octets to drop to zero), the falling alarm cannot fire because the baseline traffic is always greater than the value of the falling threshold. By definition, the failure of the falling alarm to fire prevents the rising alarm from firing a second time.

The following figure describes an alarm with a threshold less than 260.
Creating alarms

Select a variable from the variable list and a port, or other switch component, to which it is connected. Some variables require port IDs, card IDs, or other indices (for example, spanning tree group IDs). Then select a rising and a falling threshold value. The rising and falling values are compared against the actual value of the variable that you choose. If the variable falls outside of the rising or falling value range, an alarm is triggered and an event is logged or trapped.

After an alarm is created a sample type is also selected, which can be either absolute or delta. Absolute alarms are defined on the cumulative value of the alarm variable. An example of an alarm defined with absolute value is card operating status. Because this value is not cumulative, but instead represents states, such as card up (value 1) and card down (value 2), you set it for absolute value. You can create an alarm with a rising value of 2 and a falling value of 1 to alert a user to whether the card is up or down.

Most alarm variables related to Ethernet traffic are set to delta value. Delta alarms are defined based on the difference in the value of the alarm variable between the start of the polling period and the end of the polling period. Delta alarms are sampled twice for each polling period. For each sample, the last two values are added together and compared to the threshold values. This process increases precision and allows for the detection of threshold crossings that span the sampling boundary. If you track the current values of a delta-valued alarm and add them together, therefore, the result is twice the actual value. (This result is not an error in the software.)

How events work

An event specifies whether a trap, a log, or a trap and a log is generated to view alarm activity. When you enable RMON globally, two default events are generated:

- Rising Event
- Falling Event

The default events specify that after an alarm goes out of range, the firing of the alarm is tracked in both a trap and a log. For example, after an alarm triggers at the rising threshold, the rising event specifies that this information be sent to both a trap and a log. Likewise, after an alarm
passes the falling threshold, the falling event specifies that this information be sent to a trap and a log.
Chapter 4: Network monitoring configuration using ACLI

This chapter describes how to configure network monitoring using ACLI.

Navigation

- CPU utilization on page 19
- Memory utilization on page 20
- System log on page 20
- Port mirroring on page 23
- Port statistics on page 25
- Stack health on page 27

CPU utilization

Procedure steps

1. Enter Privileged exec mode.
2. To view CPU utilization for all units, enter
   `show cpu-utilization`
3. To view CPU utilization for a specific unit, enter
   `show cpu-utilization <1-8>`
4. Observe the displayed information.

Variable definitions

The following table describes the command parameters.
Memory utilization

Perform this procedure to view memory utilization.

Procedure steps

1. Enter Privileged exec mode.
2. To view memory utilization for all units, enter
   `show memory-utilization`
3. To view memory utilization for a specific unit, enter
   `show memory-utilization <1-8>`
4. Observe the displayed information.

Variable definitions

The following table describes the command parameters.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1–8&gt;</td>
<td>Specifies the number of a specific unit.</td>
</tr>
</tbody>
</table>

System log

This section describes ACLI commands that you use to configure and manage the system log.

Navigation

- Viewing the system event log on page 21
- Configuring system logging on page 21
- Disabling logging on page 22
- Disabling logging on page 22
Viewing the system event log

Prerequisites

Enter the Privileged EXEC mode

Use the **show logging** command to display the configuration and the current contents of the system event log.

Procedure steps

At the prompt, enter

```
show logging
```

Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Display the configuration of event logging.</td>
</tr>
<tr>
<td>critical</td>
<td>Display critical log messages.</td>
</tr>
<tr>
<td>informational</td>
<td>Display informational log messages.</td>
</tr>
<tr>
<td>serious</td>
<td>Display serious log messages.</td>
</tr>
<tr>
<td>sort-reverse</td>
<td>Display informational log messages in reverse chronological order (beginning with most recent).</td>
</tr>
<tr>
<td>unit</td>
<td>Display log messages for a certain unit.</td>
</tr>
</tbody>
</table>

Configuring system logging

Prerequisites

Enter Global Configuration mode.

Use the **logging** command to configure the system settings for the system event log.

Procedure steps

At the prompt, enter

```
```
logging [enable|disable] [level critical|serious|informational|none] [nv-level critical|serious|none] remote [address|enable|level] volatile [latch|overwrite]

Variable definitions

The following table describes the command parameters.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>level critical</td>
<td>serious</td>
</tr>
<tr>
<td>nv-level critical</td>
<td>serious</td>
</tr>
<tr>
<td>remote</td>
<td>Configure remote logging parameters. Address: configure remote syslog address. Enable: enable remote logging. Level: configure remote logging level.</td>
</tr>
<tr>
<td>volatile</td>
<td>Configure options for logging to DRAM. Latch: latch DRAM log after it is full. Overwrite: overwrite DRAM log after it is full.</td>
</tr>
</tbody>
</table>

Disabling logging

Prerequisites

Enter Global Configuration mode
Perform this procedure to disable the system event log.

Procedure steps

Enter

no logging

Setting default logging

Prerequisites

Enter Global Configuration mode
Perform this procedure to designate the factory default settings as the system settings for the system event log.
Clearing log messages

Prerequisites

Enter Privileged EXEC mode
Perform this procedure to clear all log messages in DRAM.

Procedure steps

At the prompt, enter

clear logging [non-volatile] [nv] [volatile]

Variable definitions

The following table describes the command parameters.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>non-volatile</td>
<td>Clear log messages from NVRAM.</td>
</tr>
<tr>
<td>nv</td>
<td>Clear log messages from NVRAM and DRAM.</td>
</tr>
<tr>
<td>volatile</td>
<td>Clear log messages from DRAM.</td>
</tr>
</tbody>
</table>

Port mirroring

This section describes how to configure and display port mirroring

- Displaying the port-mirroring configuration on page 24
- Configuring port-mirroring on page 24
- Disabling port-mirroring on page 25
Displaying the port-mirroring configuration

Prerequisites

Enter Privileged exec mode
Use this command to display the configuration and the current contents of the system event log.

Procedure steps

At the prompt, enter

show port-mirroring

Job aid

The following figure shows the command output.

![Port-mirroring command output](Figure 3: Port-mirroring command output)

Configuring port-mirroring

Prerequisites

Enter Privileged exec mode
Perform this procedure to configure port mirroring.

Procedure steps

At the prompt, enter

`port-mirroring mode {disable|Xrx|Xtx|XrxOrXtx} monitor-port <portlist> mirror-port-X <portlist>`

Variable definitions

The following table describes the command variables.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables port-mirroring.</td>
</tr>
<tr>
<td>Xrx</td>
<td>Mirror packets received on port X.</td>
</tr>
</tbody>
</table>
## Disabling port-mirroring

### Prerequisites
Enter Privileged exec mode
Perform this procedure to disable port mirroring.

### Procedure steps
At the prompt, enter

```
no port-mirroring
```

## Port statistics

This section contains information about how you can display the statistics for a port for both received and transmitted traffic.

### Navigation
- [Displaying port-statistics](#) on page 25
- [Clearing statistical information](#) on page 26

## Displaying port-statistics

### Prerequisites
Enter Interface configuration mode
Perform this procedure to display port statistics.

### Procedure steps
At the prompt, enter

```
```
show port-statistics [port <portlist>]

Variable definitions

The following table describes the command variables.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>port &lt;portlist&gt;</td>
<td>Specifies the port numbers to display statistics about.</td>
</tr>
</tbody>
</table>

⚠️ Important:
If you omit this parameter, the system uses the port number you specified when selecting the interface.

Job aid

The following image is an example of the command output.

```
show port-statistics port 1/1
Received
    Packets:   0
    Multicasts:   0
    Broadcasts:   0
    Total Octets:   0
    PCS Errors:   0
    Under sized Packets:   0
    Oversized Packets:   0
    Frame Errors:   0
    Pause Frames:   0
Transmitted
    Packets:   0
    Multicasts:   0
    Broadcasts:   0
    Total Octets:   0
    Collisions:   0
    Single Collisions:   0
    Multiple Collisions:   0
    Excessive Collisions:   0
    Deferred Packets:   0
    Late Collisions:   0
    Pause Frames:   0
    64 bytes:   0
    64-127 bytes:   0
    128-255 bytes:   0
    256-511 bytes:   0
    512-1023 bytes:   0
    1024-1518 bytes:   0
    Jum no:   0
    Dropped On No Resources:   0
```

Figure 4: Port-statistics command output

Clearing statistical information

Prerequisites

Enter Interface configuration mode

Use this command to clear all statistical information for the specified port and set all counters to zero (0).
Procedure steps

At the prompt, enter

```
clear-stats [port <portlist>]
```

Variable definitions

The following table describes the command variables.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>port &lt;portlist&gt;</td>
<td>Specifies the port numbers to display statistics about.</td>
</tr>
</tbody>
</table>

⚠️ **Important:**
If you omit this parameter, the system uses the port number you specified when selecting the interface.

Stack health

This section describes how you can view and configure stack health parameters.

Navigation

- [Viewing stack health](#) on page 27
- [Viewing stack monitor information](#) on page 28
- [Configuring the stack monitor](#) on page 28

Viewing stack health

Perform this procedure to display the stack health information.

**Procedure steps**

At the prompt, enter
show stack health

Job aid

The following image is an example of the command output.

<table>
<thead>
<tr>
<th>UNIT</th>
<th>Switch Model</th>
<th>Cascade Up</th>
<th>Cascade Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (Base)</td>
<td>2526I</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>2</td>
<td>25501-PUR</td>
<td>OK</td>
<td>OK</td>
</tr>
</tbody>
</table>

Switch Units Found = 2
Stack Health Check = OK - RESILIEN
Stack Diagnosis = Stack in full resilient mode.

Figure 5: Stack health command output

Viewing stack monitor information

Perform this procedure to display the current configuration values for the stack monitor.

Procedure steps

At the prompt, enter

```
show stack-monitor
```

Configuring the stack monitor

Perform this procedure to configure the values for the stack monitor.

Procedure steps

At the prompt, enter

```
config stack-monitor {enable [stack-size <2-8>][trap-interval <30-300>]}
```

Variable definitions

The following table describes the command parameters.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable stack monitoring.</td>
</tr>
<tr>
<td>stack-size &lt;2-8&gt;</td>
<td>Set stack size to be monitored in the range of 2 to 8.</td>
</tr>
</tbody>
</table>
Disabling the stack monitor

Perform this procedure to disable the stack monitor.

Procedure steps

At the prompt, enter

```
no stack-monitor
```
Chapter 5: Network monitoring configuration using Enterprise Device Manager

This chapter describes how to use Enterprise Device Manager (EDM) to configure system logging and to display chassis and port statistics for the Avaya Ethernet Routing Switch 2500 Series.

Navigation

- Viewing CPU and memory utilization using EDM on page 31
- Switch stack information using EDM on page 32
- Viewing stack health using EDM on page 37
- Viewing the system log settings using EDM on page 38
- Viewing the Remote System Log tab using EDM on page 40
- Viewing system logs using EDM on page 41
- Port Mirroring using EDM on page 42
- Graphing chassis statistics using EDM on page 44
- Graphing port statistics using EDM on page 51
- Configuring the stack monitor using EDM on page 56
- Using the EDM MIB Web page for SNMP Get and Get-Next on page 57
- Using the EDM MIB Web page for SNMP walk on page 57

Viewing CPU and memory utilization using EDM

Perform this procedure to view both CPU and memory utilization.

Procedure steps

1. From the navigation tree, double-click Edit.
2. In the Edit tree, double-click Chassis.
3. In the Chassis tree, double-click **Chassis**.

4. In the work area, click the **CPU/Mem Utilization** tab to display a table of CPU and memory utilization information for a switch or for all members of a stack.

5. On the toolbar, you can click **Refresh** to update the data.

---

**Variable definitions**

Use the data in the following table to help you understand CPU and memory utilization.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit</td>
<td>The numerical representation of the unit.</td>
</tr>
<tr>
<td>Last10Seconds</td>
<td>CPU usage, in percentage, for the last 10 seconds.</td>
</tr>
<tr>
<td>Last1Minute</td>
<td>CPU usage, in percentage, for the last minute.</td>
</tr>
<tr>
<td>Last10Minutes</td>
<td>CPU usage, in percentage, for the last 10 minutes.</td>
</tr>
<tr>
<td>Last1Hour</td>
<td>CPU usage, in percentage, for the last hour.</td>
</tr>
<tr>
<td>Last24Hours</td>
<td>CPU usage, in percentage, for the last 24 hours.</td>
</tr>
<tr>
<td>TotalCPUUsage</td>
<td>Memory usage in megabytes.</td>
</tr>
<tr>
<td>MemoryTotalMB</td>
<td>Total memory present, in megabytes, on the unit.</td>
</tr>
<tr>
<td>MemoryAvailableMB</td>
<td>Memory remaining available on the unit.</td>
</tr>
<tr>
<td>MemoryUsedMB</td>
<td>Memory that has been used on the unit.</td>
</tr>
</tbody>
</table>

---

**Switch stack information using EDM**

The following sections describe how to observe and configure information about the switch stack.
Navigation

- Viewing stack information using EDM on page 33
- Editing stack information using EDM on page 35
- Viewing pluggable ports using EDM on page 36

Viewing stack information using EDM

View the stack information to see a description of the units that are on the stack.

Procedure steps

1. From the navigation tree, double-click Edit.
2. In the Edit tree, double-click Chassis.
3. In the Chassis tree, double-click Switch/Stack.
4. In the work area, click the Stack info tab to display the current stack information.

Variable Definitions

Use the information in the following table to help you understand the stack information display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indx</td>
<td>Indicates the line number for stack info.</td>
</tr>
<tr>
<td>Descr</td>
<td>Describes the component or subcomponent. If not available, the value is a zero length string.</td>
</tr>
<tr>
<td>Location</td>
<td>Indicates the geographic location of a component in a system modeled as a chassis, but possibly physically implemented with geographically separate devices connected to exchange management information. Chassis modeled in this manner are sometimes referred to as virtual chassis. An example value is: 4th flr wiring closet in blg A. Important: This field applies only to components that are in either the Board or Unit groups. If the information is unavailable, for example, the chassis is not modeling a virtual chassis or component is not in a Board or Unit group, the value is a zero-length string.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>If this field is applicable and is not assigned a value through a SNMP SET PDU when the row is created, the value defaults to the value of the object s5ChasComSerNum.</td>
</tr>
<tr>
<td>LstChng</td>
<td>Indicates the value of sysUpTime when it was detected that the component or sub-component was added to the chassis. If this action has not occurred since the cold or warm start of the agent, the value is zero.</td>
</tr>
<tr>
<td>AdminState</td>
<td>Indicates the state of the component or sub-component.</td>
</tr>
<tr>
<td></td>
<td>• enable: enables operation</td>
</tr>
<tr>
<td></td>
<td>• reset: resets component</td>
</tr>
<tr>
<td>OperState</td>
<td>Indicates the current operational state of the component. The possible values are</td>
</tr>
<tr>
<td></td>
<td>• other: another state</td>
</tr>
<tr>
<td></td>
<td>• notAvail: state not available</td>
</tr>
<tr>
<td></td>
<td>• removed: component removed</td>
</tr>
<tr>
<td></td>
<td>• disabled: operation disabled</td>
</tr>
<tr>
<td></td>
<td>• normal: normal operation</td>
</tr>
<tr>
<td></td>
<td>• resetInProg: reset in progress</td>
</tr>
<tr>
<td></td>
<td>• testing: performing a self test</td>
</tr>
<tr>
<td></td>
<td>• warning: operating at warning level</td>
</tr>
<tr>
<td></td>
<td>• nonFatalErr: operating at error level</td>
</tr>
<tr>
<td></td>
<td>• fatalErr: error stopped operation</td>
</tr>
<tr>
<td></td>
<td>The component type determines the allowable (and meaningful) values.</td>
</tr>
<tr>
<td>Ver</td>
<td>Indicates the version number of the component or subcomponent. If not available, the value is a zero-length string.</td>
</tr>
<tr>
<td>SerNum</td>
<td>Indicates the serial number of the component or subcomponent. If not available, the value is a zero-length string.</td>
</tr>
<tr>
<td>BaseNumPorts</td>
<td>Indicates the number of base ports of the component or subcomponent.</td>
</tr>
<tr>
<td>TotalNumPorts</td>
<td>Indicates the number of ports of the component or subcomponent.</td>
</tr>
<tr>
<td>IpAddress</td>
<td>Indicates the IP address of the component or subcomponent.</td>
</tr>
<tr>
<td>RunningSoftwareVer</td>
<td>Indicates the software version running on the switch.</td>
</tr>
</tbody>
</table>
Editing stack information using EDM

Edit the stack information to change the information about the units in the stack.

Procedure steps

1. From the navigation tree, double-click Edit.
2. In the Edit tree, double-click Chassis.
3. In the Chassis tree, double-click Switch/Stack.
4. In the work area, click the Stack info tab to display the current stack information.
5. Double click a location in a unit description to change the name of the location.
6. Type the name of the new location.
7. Double-click the Admin State in a unit description.
   An arrow appears in the cell.
8. Click the arrow.
   A box appears with two options: enable and reset.
9. Click enable or reset.
10. On the toolbar, click Apply.

Variable definitions

Use the data in the following table to help you edit stack information.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Indicates the geographic location of a component in a system modeled as a chassis, but possibly physically implemented with geographically separate devices connected to exchange management information. Chassis modeled in this manner are sometimes referred to as virtual chassis. An example value is: 4th flr wiring closet in blg A.</td>
</tr>
</tbody>
</table>

Important:
This field applies only to components that are in either the Board or Unit groups. If the information is unavailable, for
example, the chassis is not modeling a virtual chassis or component is not in a Board or Unit group, the value is a zero-length string. If this field is applicable and is not assigned a value through a SNMP SET PDU when the row is created, the value defaults to the value of the object s5ChasComSerNum.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdminState</td>
<td>Indicates the state of the component or subcomponent.</td>
</tr>
<tr>
<td></td>
<td>• enable: enables operation</td>
</tr>
<tr>
<td></td>
<td>• reset: resets component</td>
</tr>
</tbody>
</table>

### Viewing pluggable ports using EDM

View pluggable ports to see Pluggable Ports information.

#### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Switch/Stack**.
4. In the work area, click the **Stack info** tab to display the current stack information.
5. On the toolbar, click Pluggable Ports **Pluggable Ports**.
6. Observe the displayed information.

### Variable definitions

Use the data in the following table to help you understand the Pluggable Ports information.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit</td>
<td>Identifies the unit number.</td>
</tr>
<tr>
<td>Port</td>
<td>Identifies the number of the pluggable port.</td>
</tr>
<tr>
<td>PortType</td>
<td>Identifies the type of the pluggable port.</td>
</tr>
<tr>
<td>VendorName</td>
<td>Identifies the vendor’s name.</td>
</tr>
</tbody>
</table>
Viewing stack health using EDM

Perform this procedure to view stack health information.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Switch/Stack**.
4. In the work area, click the **Stack Health** tab to display the stack health.

Variable definitions

Use the data in the following table to help you understand the stack health.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Units Found</td>
<td>Indicates the number of switch units in the stack.</td>
</tr>
<tr>
<td>Stack Health Check</td>
<td>Indicates the stack health.</td>
</tr>
<tr>
<td>Stack Diagnosis</td>
<td>Indicates the stack mode.</td>
</tr>
</tbody>
</table>
Viewing the system log settings using EDM

Perform this procedure to view System Log Settings information.

Procedure steps

1. From the navigation tree, double-click Edit.
2. In the Edit tree, double-click Diagnostics.
3. In the Diagnostics tree, double-click System Log.
4. In the work area, click the System Log Settings tab to display the system log settings.

Variable definitions

Use the data in the following table to help you understand System Log Settings information.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Enables you to store or discard generated log messages. When you specify on, the system stores log messages in the log message buffer facility according to the parameters specified by related management objects. When you specify off, the system discontinues log message accumulation. <strong>Important:</strong> This does not affect operation of the remote syslog facility, it only determines whether log messages are stored locally.</td>
</tr>
<tr>
<td>BufferFullAction</td>
<td>Specifies the action to take when buffer space is exhausted. Overwrite causes the previous messages to be overwritten. Messages are overwritten based on First In First Out (FIFO). Specifying latch causes no more messages to be saved until this object is changed to overwrite or until the buffer space is made available through some other means (for example, clearing the buffer).</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Volatile—CurSize</td>
<td>Displays the current number of log messages in the volatile portion of the system log message facility. Messages that are classified as volatile are lost upon system reinitialization.</td>
</tr>
<tr>
<td>Volatile—SaveTargets</td>
<td>Determines the type of log messages that are saved in the log message buffer facilities. Messages are classified based on their type as follows:</td>
</tr>
<tr>
<td></td>
<td>• critical</td>
</tr>
<tr>
<td></td>
<td>• critical/serious</td>
</tr>
<tr>
<td></td>
<td>• critical/serious/inform</td>
</tr>
<tr>
<td></td>
<td>• none</td>
</tr>
<tr>
<td></td>
<td>Selecting the type causes all log messages with an associated value less than or equal to the type value specified to be saved after the log message is entered into the system.</td>
</tr>
<tr>
<td></td>
<td>For example, specifying the value critical causes only messages classified as critical to be saved to nonvolatile storage. Specifying critical/serious causes critical and serious messages to be saved. Specifying a value of none means no log messages are stored in volatile memory.</td>
</tr>
<tr>
<td>non-Volatile—CurSize</td>
<td>Displays the current number of log messages that are present in the nonvolatile portion of the system log message facility. Messages that are classified as nonvolatile are saved across system reinitializations.</td>
</tr>
<tr>
<td>non-Volatile—SaveTargets</td>
<td>Determines the type of log messages that are saved to nonvolatile storage after they occur. Messages are classified based on their type as follows:</td>
</tr>
<tr>
<td></td>
<td>• critical</td>
</tr>
<tr>
<td></td>
<td>• critical/serious</td>
</tr>
<tr>
<td></td>
<td>• none</td>
</tr>
<tr>
<td></td>
<td>When you select a value the system saves all log messages with a value less than or equal to the specified value when the log message is entered into the system.</td>
</tr>
<tr>
<td></td>
<td>For example, specifying critical, causes only messages classified as critical to be saved to nonvolatile storage. Specifying critical/serious causes critical and serious messages to be saved. Specifying none causes no messages to be saved.</td>
</tr>
<tr>
<td>Action—ClearMessageBuffers</td>
<td>Indicates that the messages currently saved in the log message buffer that match the specified type are to be deleted. All messages of types matching the specified value are deleted.</td>
</tr>
</tbody>
</table>
Variable values are deleted. For example, specifying `volInformational` deletes all informational messages and specifying `nonVolCritical` deletes all critical messages from nonvolatile storage.

### Viewing the Remote System Log tab using EDM

Perform this procedure to view Remote System Log information.

**Procedure steps**

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **System Log**.
4. In the work area, click the **Remote System Log** tab to display the Remote System Log information.

### Variable definitions

Use the data in the following table to help you understand Remote System Log information.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RemoteSyslogAddressTyp</td>
<td>Specifies the IP address type of the remote system.</td>
</tr>
<tr>
<td>RemoteSyslogAddress</td>
<td>Specifies the IP address of the remote system.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Determines whether remote logging is enabled or disabled.</td>
</tr>
</tbody>
</table>
| SaveTargets               | Determines the type of log messages that are saved in the log message buffer facilities. Messages are classified based on their type as follows:  
  • critical  
  • critical/serious  
  • critical/serious/inform  
  • none  
  Selecting a type of critical, critical/serious, or critical/serious/inform causes all log messages with the specified type to be saved after the log message is entered into the system. For example, specifying the value critical causes only messages classified as critical to be sent to the remote system. |
Viewing system logs using EDM

View the system logs to view System Logs information.

Procedure steps

1. From the navigation tree, double-click Edit.
2. In the Edit tree, double-click Diagnostics.
3. In the Diagnostics tree, double-click System Log.
4. In the work area, click the System Logs tab to display the System Logs information.

Variable definitions

Use the data in the following table to help you understand the System Logs information.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OrigUnitNumber</td>
<td>Specifies the unit number of the originator of the log message.</td>
</tr>
<tr>
<td>MsgTime</td>
<td>Specifies the time (in hundredths of a second) between system initialization and the time this log message was entered into the system.</td>
</tr>
<tr>
<td>MsgIndex</td>
<td>Specifies the arbitrary integer index assigned to the log message upon entry into the message facility.</td>
</tr>
<tr>
<td>MsgSrc</td>
<td>Specifies the message source that indicates whether this message is loaded from non-volatile storage at system initialization or whether the message is generated after that time.</td>
</tr>
<tr>
<td>MsgString</td>
<td>Specifies a printable string indicating the originator of and the reason why a log message is critical/serious.</td>
</tr>
</tbody>
</table>
Port Mirroring using EDM

The following sections describe Port Mirroring.

Navigation

- Viewing Port Mirroring using EDM on page 42
- Configuring Port Mirroring using EDM on page 43

Viewing Port Mirroring using EDM

View Port Mirroring to troubleshoot the network.

Procedure steps

1. From the navigation tree, double-click Edit.
2. In the Edit tree, double-click Diagnostics.
3. In the Diagnostics tree, double-click Port Mirrors.

Variable definitions

Use the data in the following table to help you configure Port Mirroring.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Indicates the Port Mirroring instance number. Release 4.3 supports only 1 instance.</td>
</tr>
<tr>
<td>PortMode</td>
<td>Indicates the supported Port Mirroring modes. The modes are:</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• Xrx—monitors all traffic received on port X.</td>
</tr>
<tr>
<td></td>
<td>• XrxOrXtx—monitors all traffic received or transmitted on port X.</td>
</tr>
<tr>
<td></td>
<td>• Xtx—monitors all traffic transmitted on port X.</td>
</tr>
<tr>
<td>MonitorPort</td>
<td>Indicates the switch port to designate as the monitor port.</td>
</tr>
<tr>
<td>PortListX</td>
<td>Indicates the switch port to be monitored by the designated monitor port. This port is monitored according to the value X in the Monitoring Mode field.</td>
</tr>
</tbody>
</table>

## Configuring Port Mirroring using EDM

Configure Port Mirroring to help you troubleshoot the network.

### Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the **Diagnostics** tree, double-click **Port Mirrors**.
3. On the toolbar, click **Insert**.
   
   The Insert Port Mirrors dialog box appears.
4. In the **instance** box, type 1.
5. In the **PortMode** section, click one of the option buttons.
6. Beside the **MonitorPort** box, click the elipsis (...).
   
   The Port Editor: Monitor Port list appears.
7. Click a port.
8. Click **Ok**.
9. Beside the dimmed **PortListX** box, click the elipsis (...).
   
   The Port Editor: portListX list appears.
10. Click a port.
11. Click **Ok**.
12. Click **Insert**.
Variable definitions

Use the data in the following table to help you configure Port Mirroring.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Specifies the Port Mirroring instance number. Release 4.3 supports only 1 instance.</td>
</tr>
<tr>
<td>PortMode</td>
<td>Specifies the supported Port Mirroring modes. The modes are:</td>
</tr>
<tr>
<td></td>
<td>• Xrx—monitors all traffic received on port X.</td>
</tr>
<tr>
<td></td>
<td>• XrxOrXtx—monitors all traffic received or transmitted on port X.</td>
</tr>
<tr>
<td></td>
<td>• Xtx—monitors all traffic transmitted on port X.</td>
</tr>
<tr>
<td>MonitorPort</td>
<td>Specifies the switch port to designate as the monitor port.</td>
</tr>
<tr>
<td>PortListX</td>
<td>Specifies the switch port to be monitored by the designated monitor port. This port is monitored according to the value X in the Monitoring Mode field.</td>
</tr>
</tbody>
</table>

Graphing chassis statistics using EDM

Perform this procedure to graph chassis statistics

Procedure steps

1. From the navigation tree, double-click Graph.
2. In the Graph tree, double-click Chassis. The Graph Chassis dialog box appears with the SNMP tab displayed.
3. Click a row of data to graph under a column heading.
4. On the toolbar, click the Poll Interval and select an interval.
5. On the toolbar, you can reset the data by clicking Clear Counters.
6. On the toolbar, click a graph type.
The following sections contain information about the Graph Chassis dialog box tabs with descriptions of the statistics on each tab.

- **Viewing IP statistics** on page 45
- **Viewing ICMP In statistics** on page 47
- **Viewing ICMP Out statistics** on page 48
- **Viewing TCP statistics** on page 49
- **Viewing UDP statistics** on page 50

For more information about the SNMP tab, see *Avaya Ethernet Routing Switch 2500 Series Security — Configuration and Management, NN47215-505*.

---

**Viewing IP statistics**

Perform this procedure to view and graph IP statistics.

**Procedure steps**

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **IP** tab.
4. Click a row of data to graph under a column heading.
5. On the toolbar, click the **Poll Interval** and select an interval.
6. On the toolbar, you can reset the data by clicking **Clear Counters**.
7. On the toolbar, click a graph type to graph the IP statistics.

**Variable definitions**

Use the data in the following table to help you understand IP statistics.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>InReceives</td>
<td>The total number of input datagrams received from interfaces, including those received in error.</td>
</tr>
<tr>
<td>InHdrErrors</td>
<td>The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options.</td>
</tr>
<tr>
<td>InAddrErrors</td>
<td>The number of input datagrams discarded because the IP address in the IP header destination field was not a valid address. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For addresses that are not IP Gateways and therefore</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ForwDatagrams</td>
<td>The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. For addresses that do not act as IP Gateways, this counter includes only those packets Source-Routed by way of this address with successful Source-Route option processing.</td>
</tr>
<tr>
<td>InUnknownProtos</td>
<td>The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.</td>
</tr>
<tr>
<td>InDiscards</td>
<td>The number of input IP datagrams for which no problems are encountered to prevent their continued processing, but that are discarded (for example, for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.</td>
</tr>
<tr>
<td>InDelivers</td>
<td>The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).</td>
</tr>
<tr>
<td>OutRequests</td>
<td>The total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in ipForwDatagrams.</td>
</tr>
<tr>
<td>OutDiscards</td>
<td>The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that are discarded (for example, for lack of buffer space). This counter can include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.</td>
</tr>
<tr>
<td>OutNoRoutes</td>
<td>The number of IP datagrams discarded because no route can be found to transmit them to their destination. This counter also includes any packets counted in ipForwDatagrams that have no route. This includes any datagrams a host cannot route because all of its default gateways are down.</td>
</tr>
<tr>
<td>FragOKs</td>
<td>The number of IP datagrams successfully fragmented at this entity.</td>
</tr>
<tr>
<td>FragFails</td>
<td>The number of IP datagrams that are discarded because they need to be fragmented at this entity but cannot be, for example, because their Don’t Fragment flag was set.</td>
</tr>
<tr>
<td>FragCreates</td>
<td>The number of generated IP datagram fragments because of a fragmentation at this entity.</td>
</tr>
<tr>
<td>ReasmReqds</td>
<td>The number of IP fragments received that needed to be reassembled at this entity.</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ReasmOKs</td>
<td>The number of IP datagrams successfully reassembled.</td>
</tr>
<tr>
<td>ReasmFails</td>
<td>The number of failures detected by the IP reassembly algorithm (for example, timed out, errors). This is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC815) can lose track of the number of fragments by combining them as they are received.</td>
</tr>
</tbody>
</table>

**Viewing ICMP In statistics**

Perform this procedure to open the ICMP In tab to view and graph ICMP In statistics.

**Procedure steps**

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **ICMP In** tab.
4. Click a row of data to graph under a column heading.
5. On the toolbar, click the **Poll Interval** and select an interval.
6. On the toolbar, you can reset the data by clicking **Clear Counters**.
7. On the toolbar, click a graph type.

**Variable definitions**

Use the data in the following table to help you understand ICMP In statistics.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SrcQuenchs</td>
<td>The number of ICMP Source Quench messages received.</td>
</tr>
<tr>
<td>Redirects</td>
<td>The number of ICMP Redirect messages received.</td>
</tr>
<tr>
<td>Echos</td>
<td>The number of ICMP Echo (request) messages received.</td>
</tr>
<tr>
<td>EchoReps</td>
<td>The number of ICMP Echo Reply messages received.</td>
</tr>
<tr>
<td>Timestamps</td>
<td>The number of ICMP Timestamp (request) messages received.</td>
</tr>
<tr>
<td>TimestampReps</td>
<td>The number of ICMP Timestamp Reply messages received.</td>
</tr>
<tr>
<td>AddrMasks</td>
<td>The number of ICMP Address Mask Request messages received.</td>
</tr>
<tr>
<td>AddrMaskReps</td>
<td>The number of ICMP Address Mask Reply messages received.</td>
</tr>
<tr>
<td>ParmProbs</td>
<td>The number of ICMP Parameter Problem messages received.</td>
</tr>
</tbody>
</table>
Variable | Value |
---|---
DestUnreachs | The number of ICMP Destination Unreachable messages received. |
TimeExcds | The number of ICMP Time Exceeded messages received. |

### Viewing ICMP Out statistics

Perform this procedure to open the ICMP Out tab and view and graph statistics.

**Procedure steps**

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **ICMP Out** tab.
4. Click a row of data to graph under a column heading.
5. On the toolbar, click the **Poll Interval** and select an interval.
6. On the toolbar, you can reset the data by clicking **Clear Counters**.
7. On the toolbar, click a graph type.

### Variable definitions

Use the data in the following table to help you understand ICMP Out statistics.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SrcQuenchs</td>
<td>The number of ICMP Source Quench messages sent.</td>
</tr>
<tr>
<td>Redirects</td>
<td>The number of ICMP Redirect messages received. For a host, this object is always zero because hosts do not send redirects.</td>
</tr>
<tr>
<td>Echos</td>
<td>The number of ICMP Echo (request) messages sent.</td>
</tr>
<tr>
<td>EchoReps</td>
<td>The number of ICMP Echo Reply messages sent.</td>
</tr>
<tr>
<td>Timestamps</td>
<td>The number of ICMP Timestamp (request) messages sent.</td>
</tr>
<tr>
<td>TimestampReps</td>
<td>The number of ICMP Timestamp Reply messages sent.</td>
</tr>
<tr>
<td>AddrMasks</td>
<td>The number of ICMP Address Mask Request messages sent.</td>
</tr>
<tr>
<td>AddrMaskReps</td>
<td>The number of ICMP Address Mask Reply messages sent.</td>
</tr>
<tr>
<td>ParmProbs</td>
<td>The number of ICMP Parameter Problem messages sent.</td>
</tr>
<tr>
<td>DestUnreachs</td>
<td>The number of ICMP Destination Unreachable messages sent.</td>
</tr>
<tr>
<td>TimeExcds</td>
<td>The number of ICMP Time Exceeded messages sent.</td>
</tr>
</tbody>
</table>
Viewing TCP statistics

Perform this procedure to open the TCP tab and view and graph TCP statistics.

**Procedure steps**

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **TCP** tab.
4. Click a row of data to graph under a column heading.
5. On the toolbar, click the **Poll Interval** and select an interval.
6. On the toolbar, you can reset the data by clicking **Clear Counters**.
7. On the toolbar, click a graph type.

**Variable definitions**

Use the data in the following table to help you understand TCP statistics.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveOpens</td>
<td>The number of times TCP connections make a direct transition to the SYN-SENT state from the CLOSED state.</td>
</tr>
<tr>
<td>PassiveOpens</td>
<td>The number of times TCP connections make a direct transition to the SYN-RCVD state from the LISTEN state.</td>
</tr>
<tr>
<td>AttemptFails</td>
<td>The number of times TCP connections make a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections make a direct transition to the LISTEN state from the SYN-RCVD state.</td>
</tr>
<tr>
<td>EstabResets</td>
<td>The number of times TCP connections make a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.</td>
</tr>
<tr>
<td>CurrEstab</td>
<td>The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.</td>
</tr>
<tr>
<td>InSegs</td>
<td>The total number of segments received, including those received in error. This count includes segments received on currently established connections.</td>
</tr>
<tr>
<td>OutSegs</td>
<td>The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.</td>
</tr>
</tbody>
</table>
### Variable definitions

Use the data in the following table to understand the UDP statistics.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>InDatagrams</td>
<td>The total number of UDP datagrams delivered to UDP users.</td>
</tr>
<tr>
<td>NoPorts</td>
<td>The total number of received UDP datagrams for which there was no application at the destination port.</td>
</tr>
<tr>
<td>InErrors</td>
<td>The number of received UDP datagrams that cannot be delivered for reasons other than the lack of an application at the destination port.</td>
</tr>
</tbody>
</table>

---

### Viewing UDP statistics

Perform this procedure to open the UDP tab and view and graph UDP statistics.

**Procedure steps**

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **UDP** tab.
4. Click a row of data to graph under a column heading.
5. On the toolbar, click the **Poll Interval** and select an interval.
6. On the toolbar, you can reset the data by clicking **Clear Counters**.
7. On the toolbar, click a graph type.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OutDatagrams</td>
<td>The total number of UDP datagrams sent from this entity.</td>
</tr>
<tr>
<td>HCInDatagrams</td>
<td>The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.</td>
</tr>
<tr>
<td>HCOOutDatagrams</td>
<td>The number of UDP datagrams sent from this entity, for devices that can transmit more than 1 million UDP datagrams for each second. Discontinuities in the value of this counter can occur at reinitialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime.</td>
</tr>
</tbody>
</table>

**Graphing port statistics using EDM**

You can graph the following types of statistics for a port:

- AbsoluteValue
- Cumulative
- Average/sec
- Minimum/sec
- Maximum/sec
- LastVal/sec

Perform this procedure to open the graphPort dialog box for graphing.

**Procedure steps**

1. On the Device Physical View, click on the port you want to graph.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the tab for the data type you want to view and graph.
5. Click a row of data to graph under a column heading.
6. On the toolbar, click the **Poll Interval** and select an interval.
7. On the toolbar, you can reset the data by clicking **Clear Counters**.
8. On the toolbar, click a graph type.

**Graphing interface statistics**

Perform this procedure to display and graph interface parameters for a port.
Procedure steps

1. On the Device Physical View, click on a port.
2. From the navigation tree, double-click Graph.
3. In the Graph tree, double-click Port.
4. In the work area, click the Interface tab.
5. Click a row of data to graph under a column heading.
6. On the toolbar, click the Poll Interval and select an interval.
7. On the toolbar, you can reset the data by clicking Clear Counters.
8. On the toolbar, click a graph type.

Variable definitions

Use the data in the following table to help you understand interface statistics.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>InOctets</td>
<td>The total number of octets received on the interface, including framing characters.</td>
</tr>
<tr>
<td>OutOctets</td>
<td>The total number of octets transmitted out of the interface, including framing characters.</td>
</tr>
<tr>
<td>InUcastPkts</td>
<td>The number of packets delivered by this sublayer to a higher sublayer that are not addressed to a multicast or broadcast address at this sublayer.</td>
</tr>
<tr>
<td>OutNUcastPkts</td>
<td>The total number of packets that higher-level protocols requested be transmitted, and that are addressed to a multicast or broadcast address at this sublayer, including those that are discarded or not sent.</td>
</tr>
<tr>
<td>InMulticastPkts</td>
<td>The number of packets delivered by this sublayer to a higher sublayer that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both group and functional addresses.</td>
</tr>
<tr>
<td>OutMulticastPkts</td>
<td>The number of packets that higher-level protocols requested be transmitted, and that are addressed to a multicast address at this sublayer, including those that were discarded or not sent. For a MAC layer protocol, this number includes both group and functional addresses.</td>
</tr>
<tr>
<td>InBroadcastPkts</td>
<td>The number of packets delivered by this sublayer to a higher sublayer that are addressed to a broadcast address at this sublayer.</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OutBroadcastPkts</td>
<td>The number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this sublayer, including those that were discarded or not sent.</td>
</tr>
<tr>
<td>InDiscards</td>
<td>The number of inbound packets chosen to be discarded even though no errors were detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet can be to free up buffer space.</td>
</tr>
<tr>
<td>OutDiscards</td>
<td>The number of outbound packets chosen to be discarded even though no errors were detected to prevent their being transmitted. One possible reason for discarding such a packet can be to free up buffer space.</td>
</tr>
<tr>
<td>InErrors</td>
<td>For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.</td>
</tr>
<tr>
<td>OutErrors</td>
<td>For packet-oriented interfaces, the number of outbound packets that cannot be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that cannot be transmitted because of errors.</td>
</tr>
<tr>
<td>InUnknownProtos</td>
<td>For packet-oriented interfaces, the number of packets received through the interface that are discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received through the interface that are discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter is always zero.</td>
</tr>
</tbody>
</table>

**Graphing the Ethernet error statistics**

Perform this procedure to view and graph Ethernet error statistics.

**Procedure steps**

1. On the Device Physical View, click on a port.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **Ethernet Errors** tab.
5. Click a row of data to graph under a column heading.
6. On the toolbar, click the **Poll Interval** and select an interval.
7. On the toolbar, you can reset the data by clicking **Clear Counters**.
8. On the toolbar, click a graph type.

**Variable definitions**

Use the data in the following table to help you understand the Ethernet error statistics.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlignmentErrors</td>
<td>A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the AlignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</td>
</tr>
<tr>
<td>FCSErrors</td>
<td>A count of frames received on a particular interface that are an integral number of octets in length, but do not pass the FCS check. The count represented by an instance of this object is incremented when the FCSErrors status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</td>
</tr>
<tr>
<td>InternalMacTransmitErrors</td>
<td>A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object.</td>
</tr>
<tr>
<td>InternalMacReceiveErrors</td>
<td>A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object. The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object can represent a count of receive errors on a particular interface that are not otherwise counted.</td>
</tr>
<tr>
<td>CarrierSenseErrors</td>
<td>The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>this object is incremented at most once for each transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.</td>
<td></td>
</tr>
<tr>
<td>FrameTooLongs</td>
<td>A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the FrameTooLongs status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</td>
</tr>
<tr>
<td>SQETestErrors</td>
<td>A count of times that the SQE Test Errors message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.</td>
</tr>
<tr>
<td>DeferredTransmissions</td>
<td>A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.</td>
</tr>
<tr>
<td>SingleCollisionFrames</td>
<td>A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object.</td>
</tr>
<tr>
<td>MultipleCollisionFrames</td>
<td>A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.</td>
</tr>
<tr>
<td>LateCollisions</td>
<td>The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.</td>
</tr>
<tr>
<td>ExcessiveCollisions</td>
<td>A count of frames for which transmission on a particular interface fails due to excessive collisions.</td>
</tr>
</tbody>
</table>
Graphing miscellaneous statistics

Perform this procedure to view and graph statistics from the Misc. Stats tab.

Procedure steps

1. On the Device Physical View, click on a port.
2. From the navigation tree, double-click Graph.
3. In the Graph tree, double-click Port.
4. In the work area, click the Misc. Stats tab.
5. Click a row of data to graph under a column heading.
6. On the toolbar, click the Poll Interval and select an interval.
7. On the toolbar, you can reset the data by clicking Clear Counters.
8. On the toolbar, click a graph type.

Variable definitions

Use the data in the following table to help you understand miscellaneous statistics.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NoResourcesPktsDropped</td>
<td>The number of packets dropped due to switch memory shortage.</td>
</tr>
</tbody>
</table>

Configuring the stack monitor using EDM

Perform this procedure to configure stack monitor parameters with EDM.

Procedure steps

1. From the navigation tree, double-click Edit.
2. In the Edit tree, double-click Chassis.
3. In the Chassis tree, double-click Chassis.
4. In the work area, click the Stack Monitor tab.
5. On the Stack Monitor tab, enter the required parameters.
6. On the toolbar, click Apply.
Variable definitions

Use the data in the following table to help you configure the stack monitor.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>StackErrorNotificationEnabled</td>
<td>Enable or disable stack monitoring.</td>
</tr>
<tr>
<td>ExpectedStackSize</td>
<td>Set stack size to be monitored in the range of 2 to 8.</td>
</tr>
<tr>
<td>StackErrorNotificationInterval</td>
<td>Set interval between traps in the range of 30 to 300 Seconds.</td>
</tr>
</tbody>
</table>

Using the EDM MIB Web page for SNMP Get and Get-Next

You can use the EDM Management Information Base (MIB) Web page to view the response of an SNMP Get and Get-Next request for any Object Identifier (OID).

Procedure steps

1. From the navigation tree, double-click Administration.
2. In the Administration tree, double-click MIB Web Page.
3. In the MIB Name/ OID box, enter the object name or OID.
4. Click Get.
   The result of the request appears in the Result area of the window. If the request is unsuccessful, a description of the received error appears.
5. Click Get Next to retrieve the information of the next object in the MIB.
6. Repeat step 3 as required.

Using the EDM MIB Web page for SNMP walk

You can use SNMP walk to retrieve a subtree of the MIB that has the SNMP object as root.

Perform this procedure to request the result of MIB Walk.

Procedure steps

1. From the navigation tree, double-click Administration.
2. In the Administration tree, double-click MIB Web Page.
3. In the **MIB Name/ OID** box, enter the object name or OID.

4. Click **Walk**.

   The result of the request appears in the Result area. If the request is unsuccessful, a description of the received error appears.
Chapter 6: RMON using ACLI

This section describes ACLI commands used to configure and manage RMON. For details see the following section:

- Viewing the RMON alarms on page 59
- Viewing the RMON events on page 60
- Viewing the RMON history on page 60
- Viewing the RMON statistics on page 60
- Viewing RMON history for a port on page 61
- Viewing RMON packets for a port on page 61
- Viewing RMON statistics for a port on page 62
- Configuring RMON alarms on page 62
- Deleting RMON alarms on page 63
- Configuring RMON events settings on page 64
- Deleting RMON events settings on page 65
- Configuring RMON history settings on page 65
- Deleting RMON history settings on page 66
- Configuring RMON statistics settings on page 66
- Deleting RMON statistics on page 67

Viewing the RMON alarms

Prerequisites

Enter Global Configuration mode

Perform this procedure to display information about RMON alarms.

Procedure steps

At the prompt, enter
show rmon alarm

---

### Viewing the RMON events

**Prerequisites**

Enter Global Configuration mode

Perform this procedure to display information about RMON events.

**Procedure steps**

At the prompt, enter

```
show rmon event
```

---

### Viewing the RMON history

**Prerequisites**

Enter Global Configuration mode

Perform this procedure to display information about the configuration of RMON history.

**Procedure steps**

At the prompt, enter

```
show rmon history
```

---

### Viewing the RMON statistics

**Prerequisites**

Enter Global Configuration mode

Perform this procedure to display information about the configuration of RMON statistics.

**Procedure steps**

At the prompt, enter
show rmon stats

---

**Viewing RMON history for a port**

**Prerequisites**

Enter Global Configuration mode  
Perform this procedure to display RMON history for a port.

**Procedure steps**

At the prompt, enter

```
show rmon ethernet history port LINE
```

---

**Variable definitions**

The following table describes the parameters for this command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINE</td>
<td>Specifies a list of ports</td>
</tr>
</tbody>
</table>

---

**Viewing RMON packets for a port**

**Prerequisites**

Enter Global Configuration mode  
Perform this procedure to display RMON packets for a port.

**Procedure steps**

1. To view RMON packets for all ports, enter

   ```
   show rmon ethernet packets
   ```

2. To view RMON packets for a specific port, enter

   ```
   show rmon ethernet packets port LINE
   ```
Variable definitions

The following table describes the parameters for this command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINE</td>
<td>Specifies a list of ports</td>
</tr>
</tbody>
</table>

Viewing RMON statistics for a port

Prerequisites

Enter Global Configuration mode

Perform this procedure to display RMON statistics for a port.

Procedure steps

1. To view RMON statistics for all ports, enter
   `show rmon ethernet statistics`
2. To view RMON statistics for a specific port, enter
   `show rmon ethernet statistics port LINE`

Variable definitions

The following table describes the parameters for this command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINE</td>
<td>Specifies a list of ports</td>
</tr>
</tbody>
</table>

Configuring RMON alarms

Prerequisites

Enter Global Configuration mode

Perform this procedure to set RMON alarms and thresholds.
Procedure steps

At the prompt, enter

```
rmon alarm <1-65535> <WORD> <1-2147483647> {absolute | delta} rising-threshold <-2147483648-2147483647> [1-65535>] falling-threshold <-2147483648-2147483647> [1-65535>] [owner <LINE>]```

Variable definitions

The following table describes the parameters for this command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Unique index for the alarm entry.</td>
</tr>
<tr>
<td>&lt;WORD&gt;</td>
<td>The MIB object to be monitored. This is an object identifier, and for most available objects, an English name can be used.</td>
</tr>
<tr>
<td>&lt;1-2147483647&gt;</td>
<td>The sampling interval, in seconds.</td>
</tr>
<tr>
<td>absolute</td>
<td>Use absolute values (value of the MIB object is compared directly with thresholds).</td>
</tr>
<tr>
<td>delta</td>
<td>Use delta values (change in the value of the MIB object between samples is compared with thresholds).</td>
</tr>
<tr>
<td>rising-threshold</td>
<td>The first integer value is the rising threshold value. The optional second integer specifies the event entry to be triggered when the rising threshold is crossed. If omitted, or if an invalid event entry is referenced, no event is triggered. Unique index for the alarm entry.</td>
</tr>
<tr>
<td>falling-threshold</td>
<td>The first integer value is the falling threshold value. The optional second integer specifies the event entry to be triggered when the falling threshold is crossed. If omitted, or if an invalid event entry is referenced, no event is triggered. Unique index for the alarm entry.</td>
</tr>
<tr>
<td>[owner &lt;LINE&gt;]</td>
<td>Specify an owner string to identify the alarm entry.</td>
</tr>
</tbody>
</table>

Deleting RMON alarms

Prerequisites

Enter Global Configuration mode

Perform this procedure to delete RMON alarm table entries. When the variable is omitted, all entries in the table are cleared.
Procedure steps

At the prompt, enter

    no rmon alarm [1-65535]

Variable definitions

The following table describes the command parameters.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Unique identifier of the alarm.</td>
</tr>
</tbody>
</table>

Configuring RMON events settings

Prerequisites

Enter Global Configuration mode

Perform this procedure to configure RMON event log and trap settings.

Procedure steps

At the prompt, enter

    rmon event <1-65535> [log] [trap] [description <LINE>] [owner <LINE>]

Variable definitions

The following table describes the command parameters

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Unique index for the event entry.</td>
</tr>
<tr>
<td>[log]</td>
<td>Record events in the log table.</td>
</tr>
<tr>
<td>[trap]</td>
<td>Generate SNMP trap messages for events.</td>
</tr>
<tr>
<td>[description &lt;LINE&gt;]</td>
<td>Specify a textual description for the event.</td>
</tr>
<tr>
<td>[owner &lt;LINE&gt;]</td>
<td>Specify an owner string to identify the event entry.</td>
</tr>
</tbody>
</table>
Deleting RMON events settings

Prerequisites

Enter Global Configuration mode

Perform this procedure to delete RMON event table entries. When the variable is omitted, all entries in the table are cleared.

Procedure steps

At the prompt, enter

```
no rmon alarm [<1-65535>]
```

Variable definitions

The following table describes the command parameters.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Unique identifier of the alarm.</td>
</tr>
</tbody>
</table>

Configuring RMON history settings

Prerequisites

Enter Global Configuration mode

Perform this procedure to configure RMON history settings.

Procedure steps

At the prompt, enter

```
rmon history <1-65535> <LINE> <1-65535> <1-3600> [owner <LINE>]
```

Variable definitions

The following table describes the command parameters.
### Deleting RMON history settings

**Prerequisites**

Enter Global Configuration mode

Perform this procedure to delete RMON history table entries.

**Procedure steps**

At the prompt, enter

```
no rmon history [1-65535]
```

### Variable definitions

The following table describes the command parameters.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-65535&gt;</code></td>
<td>Unique identifier of the alarm.</td>
</tr>
</tbody>
</table>

### Configuring RMON statistics settings

**Prerequisites**

Enter Global Configuration mod.

Perform this procedure to configure RMON statistics settings.

**Procedure steps**

At the prompt, enter
rmon stats <1-65535> <LINE> [owner <LINE>]

Variable definitions

The following table describes the command parameters.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Unique index for the stats entry.</td>
</tr>
<tr>
<td>[owner &lt;LINE&gt;]</td>
<td>Specify an owner string to identify the stats entry.</td>
</tr>
</tbody>
</table>

Deleting RMON statistics

Prerequisites

Enter Global Configuration mode

Perform this procedure to disable RMON statistics. When the variable is omitted, all entries in the table are cleared.

Procedure steps

At the prompt, enter

no rmon stats [<1-65535>]

Variable definitions

The following table describes the command parameters.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Unique identifier of the alarm.</td>
</tr>
</tbody>
</table>
Chapter 7: RMON using Enterprise Device Manager

The Remote Network Monitoring (RMON) MIB is an interface between the RMON agent on an Ethernet Routing Switch 2500 Series and an RMON management application, such as Enterprise Device Manager (EDM).

The RMON agent defines objects that are suitable for the management of any type of network, but some groups are targeted for Ethernet networks in particular.

The RMON agent continuously collects statistics and monitors switch performance. You can view this data through EDM.

RMON has three major functions:

• creating and displaying alarms for user-defined events
• gathering cumulative statistics for Ethernet interfaces
• tracking a history of statistics for Ethernet interfaces

Navigation

• Working with RMON information on page 69
• Creating an alarm on page 77
• Deleting an alarm on page 78
• Using RMON events on page 79
• Viewing RMON log information on page 81

Working with RMON information

You can view RMON information by reviewing the Graph information associated with the port or chassis.
**Viewing statistics**

You can use EDM to gather Ethernet statistics that you can graph in a variety of formats. You can save the statistics output to a file and export the statistics to an outside presentation or graphing application.

Perform this procedure to view RMON Ethernet statistics.

**Procedure steps**

1. On the Device Physical View, click on a port.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. Click the **Rmon** tab.
5. Click a row of data to graph under a column heading.
6. On the toolbar, click the **Poll Interval** and select an interval.
7. On the toolbar, you can reset the data by clicking **Clear Counters**.
8. On the toolbar, click a graph type.

**Variable definitions**

Use the information in the following table to help you understand RMON Ethernet statistics.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Octets</td>
<td>The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval.</td>
</tr>
<tr>
<td>Pkts</td>
<td>The total number of packets (including bad packets, broadcast packets, and multicast packets) received.</td>
</tr>
<tr>
<td>BroadcastPkts</td>
<td>The total number of good packets received that are directed to the broadcast address. This does not include multicast packets.</td>
</tr>
<tr>
<td>MulticastPkts</td>
<td>The total number of good packets received that are directed to a multicast address. This number does not include packets directed to the broadcast address.</td>
</tr>
<tr>
<td>CRCAngErrors</td>
<td>The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UndersizePkts</td>
<td>The total number of packets received that are less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.</td>
</tr>
<tr>
<td>Fragments</td>
<td>The total number of packets received that are less than 64 octets in length (excluding framing bits but including FCS octets) and with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). For etherStatsFragments to increment is normal because it counts both runts (which are normal occurrences due to collisions) and noise hits.</td>
</tr>
<tr>
<td>Collisions</td>
<td>The best estimate of the total number of collisions on this Ethernet segment.</td>
</tr>
<tr>
<td>Jabbers</td>
<td>The total number of packets received that are longer than 1518 octets (excluding framing bits, but including FCS octets), with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.</td>
</tr>
<tr>
<td>1 to 64</td>
<td>The total number of packets (including bad packets) received that are less than or equal to 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>65 to 127</td>
<td>The total number of packets (including bad packets) received that are greater than 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>128 to 255</td>
<td>The total number of packets (including bad packets) received that are greater than 127 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>256 to 511</td>
<td>The total number of packets (including bad packets) received that are greater than 255 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>512 to 1023</td>
<td>The total number of packets (including bad packets) received that are greater than 511 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>1024 to 1518</td>
<td>The total number of packets (including bad packets) received that are greater than 1023 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>OversizePkts (&gt;1518)</td>
<td>The total number of packets received that are longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.</td>
</tr>
</tbody>
</table>
Job aid

The following table describes the types of RMON statistics.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absolute</td>
<td>The total count since the last time counters were reset. A system restart resets all counters.</td>
</tr>
<tr>
<td>Cumulative</td>
<td>The total count since the statistics tab was first opened. The elapsed time for the cumulative counter appears at the bottom of the graph window.</td>
</tr>
<tr>
<td>Average/sec</td>
<td>The cumulative count divided by the cumulative elapsed time.</td>
</tr>
<tr>
<td>Min/sec</td>
<td>The minimum average for the counter for a given polling interval over the cumulative elapsed time.</td>
</tr>
<tr>
<td>Max/sec</td>
<td>The maximum average for the counter for a given polling interval over the cumulative elapsed time.</td>
</tr>
<tr>
<td>LastVal/sec</td>
<td>The average for the counter over the last polling interval.</td>
</tr>
</tbody>
</table>

Viewing RMON history

Ethernet history records periodic statistical samples from a network. A sample is called a history and is gathered in time intervals referred to as buckets. Histories establish a time-dependent method for gathering RMON statistics on a port. The default values for history are as follows:

- Buckets are gathered at 30-seconds and 30-minute intervals.
- Number of buckets gathered is 15 for the 30 seconds intervals, and 5 for the 30 minutes intervals.

You can configure both the time interval and the number of buckets. However, when the last bucket is reached, bucket 1 is dumped and recycled to hold a new bucket of statistics. Then subsequent buckets are dumped in numerical order.

Perform this procedure to view RMON history.

Procedure steps

1. From the navigation tree, double-click Rmon.
2. In the RMON tree, double-click Control.

The Rmon Control work area appears with the History tab displayed.
Creating RMON history characteristics

You can use RMON to collect statistics at intervals. For example, if you want to gather RMON statistics over the weekend, you must configure enough buckets to cover two days. To do this, set the history to gather one bucket each hour, covering the 48-hour period. After you set history characteristics, you cannot modify them; you must delete the history and create another one.

Perform this procedure to establish a history for a port and set the bucket interval.

Procedure steps

1. From the navigation tree, double-click Rmon.
2. In the RMON tree, double-click Control.
3. In the work area, click Insert to open the Insert History dialog.
4. Type the port number or click the ellipsis to select a port from the list.
5. In the Buckets Requested box, type the number of buckets, or click the ellipsis to select a value from the list. The default value is 50.
6. In the Interval box, type the length of the interval or click the ellipsis to select a value from the list. The default value is 1800.
7. In the Owner box, type the owner—the network management system that created this entry.
8. Click Insert to add the entry to the list and return to the History tab.

RMON collects statistics using the index, port, bucket, and interval that you specified.

Variable definitions

Use the data in the following table to help you create the RMON history characteristics.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>A unique value assigned to each interface. An index identifies an entry in a table.</td>
</tr>
<tr>
<td>Port</td>
<td>Any Ethernet interface on the device.</td>
</tr>
<tr>
<td>BucketsRequested</td>
<td>The requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this entry.</td>
</tr>
<tr>
<td>BucketsGranted</td>
<td>The number of discrete sampling intervals over which data is saved in the part of the media-specific table associated with this entry. The actual number of buckets associated with this entry can be less than the value of this object. In this case, at the end</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>of each sampling interval, a new bucket is added to the media-specific table.</td>
<td></td>
</tr>
<tr>
<td>Interval</td>
<td>The interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this entry. You can set this interval to any number of seconds between 1 and 3600 (1 hour). Because the counters in a bucket can overflow at their maximum value with no indication, note the possibility of overflow in any of the associated counters. Consider the minimum time in which any counter could overflow on a particular media type and set the historyControlInterval object to a value less than this interval. This minimum time is typically most important for the octets counter in any media-specific table. For example, on an Ethernet network, the etherHistoryOctets counter could overflow in about 1 hour at the maximum utilization of the Ethernet.</td>
</tr>
<tr>
<td>Owner</td>
<td>The network management system that created this entry.</td>
</tr>
</tbody>
</table>

---

**Disabling RMON history**

Perform this procedure to disable RMON history on a port.

**Procedure steps**

1. From the navigation tree, double-click **Rmon**.
2. In the RMON tree, double-click **Control**.
3. In the work area, click the row that contains the port ID you want to delete.
4. Click **Delete**.
5. On the toolbar, click **Yes** to delete the data and return to the History tab, or click **No** to return to the History tab without deleting the data.

---

**Graphing RMON history statistics**

Perform this procedure to display and graph RMON History statistics.

**Procedure steps**

1. From the navigation tree, double-click **Rmon**.
2. In the RMON tree, double-click **Control**.
3. In the work area, click a row of data to graph.
4. On the toolbar, click Display History Data.
Variable definitions

Use the data in the following table to understand the RMON History statistics.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SampleIndex</td>
<td>An index that uniquely identifies the particular sample this entry represents among all the samples associated with the same entry. This index starts at 1 and increases by one as each new sample is taken.</td>
</tr>
<tr>
<td>Utilization</td>
<td>The best estimate of the mean physical layer network utilization on this interface during the sampling interval (in hundredths of a percent).</td>
</tr>
<tr>
<td>Octets</td>
<td>The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval.</td>
</tr>
<tr>
<td>Pkts</td>
<td>The total number of packets (including bad packets, broadcast packets, and multicast packets) received.</td>
</tr>
<tr>
<td>BroadcastPkts</td>
<td>The total number of good packets received that are directed to the broadcast address. This does not include multicast packets.</td>
</tr>
<tr>
<td>MulticastPkts</td>
<td>The total number of good packets received that are directed to a multicast address. This number does not include packets directed to the broadcast address.</td>
</tr>
<tr>
<td>DropEvents</td>
<td>The total number of events in which packets are dropped by the probe due to lack of resources during this sampling. This number is not necessarily the number of packets dropped; it is the number of times this condition is detected.</td>
</tr>
<tr>
<td>CRCAErrors</td>
<td>The total number of packets received with a length (excluding framing bits, but including FCS octets) between 64 and 1518 octets, inclusive, but with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>UndersizePkts</td>
<td>The total number of packets received that are less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.</td>
</tr>
<tr>
<td>OversizePkts</td>
<td>The total number of packets received that are longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.</td>
</tr>
<tr>
<td>Fragments</td>
<td>The number of packets received during the sampling interval were less than 64 octets long (including FCS octets, but not framing bits. The packets had a bad FCS with either an integral</td>
</tr>
</tbody>
</table>
Enabling Ethernet statistics gathering

Perform this procedure to use RMON to gather Ethernet statistics.

Procedure steps

1. From the navigation tree, double-click Rmon.
2. In the Rmon tree, double-click Control.
3. In the work area, click the Ether Stats tab.
4. On the toolbar, click Insert to open the Insert Ether Stats dialog box.
5. In the Index box, type the index number or click the ellipses to select an index number from the list.
   After you enter the port number, EDM assigns an index number.
6. In the Port box, type the port number or click the ellipses to select a port from the list.
7. In the Owner box, type the owner information.
8. Click Insert.

Variable definitions

Use the data in the following table to help you gather Ethernet statistics.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>A unique value assigned to each interface. An index identifies an entry in a table.</td>
</tr>
<tr>
<td>Port</td>
<td>Any Ethernet interface on the device.</td>
</tr>
<tr>
<td>Owner</td>
<td>The network management system which created this entry.</td>
</tr>
</tbody>
</table>

Disabling Ethernet statistics gathering

Perform this procedure to disable Ethernet statistics that you have set.
Procedure steps

1. From the navigation tree, double-click **Rmon**.
2. In the Rmon tree, double-click **Control**.
3. In the work area, click the **Ether Stats** tab.
4. Click the row that contains the port ID you want to delete.
5. On the toolbar, click **Delete**.
6. Select **Yes** to delete the selected entry from the table, or click **No** to return to the Ether Stats tab without deleting the entry.

Creating an alarm

Perform this procedure to create an alarm to receive statistics and history using default values.

Procedure steps

1. From the navigation tree, double-click **Rmon**.
2. In the Rmon tree, double-click **Alarms**.
3. On the toolbar, click **Insert** to open the **Insert Alarms** dialog box.
4. Type and select the values to create the alarm.
5. Click **Insert** to add the alarm and return to the **Alarms** tab.

Variable definitions

Use the data in the following table to help you create an alarm.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable</td>
<td>Name and type of alarm—indicated by the format: alarmname.x where x=0 indicates a chassis alarm. alarmname. where the user must specify the index. The index is a card number for module-related alarms, an STG ID for spanning tree group alarms (the default STG is 1, other STG IDs are user-configured), or the Ether Statistics Control Index for RMON Stats alarms. alarmname with no dot or index is a port-related alarm and results in display of the port selection tool.</td>
</tr>
<tr>
<td>Sample Type</td>
<td>Can be either absolute or delta.</td>
</tr>
<tr>
<td>Interval</td>
<td>Time period (in seconds) over which the data is sampled and compared with the rising and falling thresholds.</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Index</td>
<td>Uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device.</td>
</tr>
<tr>
<td>Rising Threshold</td>
<td>When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, the alarm generates a single event.</td>
</tr>
<tr>
<td>RisingEventIndex</td>
<td>Index of the event entry that is used after a rising threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already entered.)</td>
</tr>
<tr>
<td>Falling Threshold</td>
<td>When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, the alarm generates a single event.</td>
</tr>
<tr>
<td>FallingEventIndex</td>
<td>Index of the event entry that is used after a falling threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already entered.)</td>
</tr>
<tr>
<td>Owner</td>
<td>The network management system which created this entry.</td>
</tr>
</tbody>
</table>

**Deleting an alarm**

Perform this procedure to delete an alarm

**Procedure steps**

1. From the navigation tree, double-click **Rmon**.
2. In the Rmon tree, double-click **Alarms**.
3. In the work area, click on a row for the alarm that you want to delete.
4. On the toolbar, click **Delete**.
5. Click **Yes** to delete the alarm and return to the **Alarms** tab, or click **No** to return to the **Alarms** tab without deleting the alarm.
Using RMON events

This section describes how RMON events and alarms work together to notify you after values in your network are outside of a specified range. When values pass the specified ranges, the alarm is triggered and it triggers. The event specifies how the activity is recorded.

Navigation

- Viewing an event on page 79
- Creating an event on page 80
- Deleting an event on page 81

Viewing an event

Perform this procedure to view a table of events.

Procedure steps

1. From the navigation tree, double-click Rmon.
2. In the Rmon tree, double-click Alarms.
3. In the work area, click the Events tab.

Variable definitions

Use the data in the following table to help you understand a table of events.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>This index uniquely identifies an entry in the event table. Each entry defines one event that is to be generated after the appropriate conditions occur.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies whether the event is a rising or a falling event.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of notification that Enterprise Device Manager provides about this event. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations. Possible notifications are as follows:</td>
</tr>
<tr>
<td></td>
<td>• none</td>
</tr>
<tr>
<td></td>
<td>• log</td>
</tr>
</tbody>
</table>
### Variable | Value
--- | ---
| • trap  
| • log-and-trap |

Community
The SNMP community string acts as a password. Only those management applications with this community string can view the alarms.

LastTimeSent
The value of sysUpTime at the time this event entry last generated an event. If this entry has not generated any events, this value is zero.

Owner
If traps are specified to be sent to the owner then this is the name of the machine that receives alarm traps.

---

## Creating an event

Perform this procedure to create an event.

### Procedure steps

1. From the navigation tree, double-click **Rmon**.
2. In the Rmon tree, double click **Alarms**.
3. In the work area, click the **Events** tab.
4. On the toolbar, click **Insert**.
5. In the **Index** box, type the index for the event.
6. In the **Description** box, type the description of the event.
7. In the **Type** section, click a type option button.

   When you designate the event type
   - to save memory you can specify the event type as **log**
   - to reduce traffic from the switch or improve CPU utilization, you can specify the event type as **snmp-trap**

   **Important:**
   If you select an event type of **snmp-trap** or **log-and-trap**, you must set trap receivers.

8. In the **Community** box, type a community.
9. In the **Owner** box, type an owner.
10. Click **Insert**.
Deleting an event

Perform this procedure to delete an event.

Procedure steps

1. From the navigation tree, double-click Rmon.
2. In the Rmon tree, double-click Alarms.
3. In the work area, click the Events tab.
4. Click a row to delete.
5. On the toolbar, click Delete.
6. Click Yes to delete the event or click No to return to the Events tab.

Viewing RMON log information

Perform this procedure to open the Log tab.

Procedure steps

1. From the navigation tree, double-click Rmon.
2. In the Rmon tree, double-click Alarms.
3. In the work area, click the Log tab.

Variable definitions

Use the data in the following table to help you open the Log tab.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The value of sysUpTime after this log entry was created.</td>
</tr>
<tr>
<td>Description</td>
<td>An implementation-dependent description of the event that activated the log entry.</td>
</tr>
<tr>
<td>EventIndex</td>
<td>Index of the event entry.</td>
</tr>
</tbody>
</table>