Avaya Ethernet Routing Switch 3500 Series Configuration — System Monitoring

5.0
NN47203-501
Issue 01.02
March 2013

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

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of 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 websites referenced within this site or documentation 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 its hardware and Software (“Product(s)”). 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 website: http://support.avaya.com. Please note that if you acquired the Product(s) 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. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

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; 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”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product 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 unless expressly authorized by Avaya. 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

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security

vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation 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 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 non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Purpose of this document

This guide provides information about system logging, displaying system statistics, and configuring network monitoring on the Avaya Ethernet Routing Switch 3500 Series. This guide describes the features of the following Avaya switches.

- Avaya Ethernet Routing Switch 3510GT
- Avaya Ethernet Routing Switch 3510GT-PWR+
- Avaya Ethernet Routing Switch 3524GT
- Avaya Ethernet Routing Switch 3524GT-PWR+
- Avaya Ethernet Routing Switch 3526T
- Avaya Ethernet Routing Switch 3526T-PWR+

The term "Ethernet Routing Switch 3500 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.

Chapter 2: New in this release

This is a new document for Avaya Ethernet Routing Switch 3500 Series Release 5.0.

The Avaya ERS 3500 Series is new and supports the following hardware and software features:

ERS 3500 hardware

The following table lists and describes the supported hardware for ERS 3500 Series 5.0. Question marks (?) in the table signify power cord types; substitute the following regional variants:

- A — no power cord
- B — EU power cord
- C — UK / Ireland power cord
- D — Japan power cord
- E — North American power cord
- F — Australia / New Zealand / China power cord

Note:

All switches support autopolarity.

Table 1: Hardware

Hardware	Description
Switch models	
AL3500?01–E6	3526T — 24 10/100BaseT ports supporting autosensing and autonegotiation, in a non-PoE , plus two 10/100/1000 or Small Form Pluggable (SFP) front combination ports, plus two SFP rear ports. Fanless.
AL3500?11–E6	3526T-PWR+ — 24 10/100BaseT PoE+ ports (802.3af/at), plus two 10/100/1000 or Small Form Pluggable (SFP) front combination ports, plus two SFP rear ports.
AL3500?04–E6	3510GT — 8 10/100/1000BaseT ports, plus two SFP ports (ports 9 and 10). Standalone and fanless.
AL3500?14–E6	3510GT-PWR+ — 8 10/100/1000BaseT PoE+ ports (802.3af/at), plus two SFP ports (ports 9 and 10). Standalone. Fanless operation in Low Power mode @ 60W max PoE budget, or normal fan

Hardware	Description
	operation in High Power mode @ 170W max PoE budget.
AL3500?05–E6	3524GT — 24 10/100/1000BaseT ports, four SFP ports shared with ports 21–24, plus two SFP rear ports.
AL3500?15–E6	3524GT-PWR+ — 24 10/100/1000BaseT PoE+ ports (802.3af/at), four SFP ports shared with ports 21–24, plus two SFP rear ports.
Rack Mount Kits	
AL3511001–E6	Spare Rack Mount Kit — this kit can be used as a replacement rack mount kit for ERS 3524GT, ERS 3524GT-PWR+, ERS 3526T or ERS 3526T-PWR + switches.
AL3511002–E6	3510–Pair Rack Mount Kit — this kit is used to connect two ERS 3510GT or ERS 3510GT-PWR+ switches together side by side and mount them in a 19 inch rack.
AL3511003–E6	3510–Single Rack Mount Kit — this kit is used to mount a single ERS 3510GT or ERS 3510GT-PWR+ switch in a standard 19 inch rack.

ERS 3500 software features

The following software features are supported on the ERS 3500 Series Release 5.0:

- BootP or Default IP
- RADIUS password fallback
- Downloading agent & diags without reset
- Username Password enhancement
- Autosave configuration enhancements
- Ping enhancement
- Writemem and save config command
- Configurable SNMP trap port (only SNMP v1 & v2)
- SNTP & SNTP timezone enhancement
- Shutdown, reload enhancement
- Factory-default command
- Show MAC address enhancement
- Show Port enhancement
- Show Running Config (verbose, non-verbose, module) enhancement

- VLAN Tagging enhancement
- 802.1AB (LLDP) Standards Based Auto Topology
- 802.1w&s — rapid and multiple spanning trees
- 802.3ad- Link Aggregation Control Protocol (LACP)
- 802.3af — Power over Ethernet (PoE)
- 802.3at — Power over Ethernet plus (PoE+)
- COS/DSCP — allows mapping the DSCP value (carried by IP frames) to 802.1p priority value
- Rate Limiting
- Remote logging — ability to log on remote servers
- Web Quick Start
- WEB HTTP download of ASCII — allows downloading of ASCII configuration files through HTTP
- HTTP web-based management
- HTTPS/SSL secure web management
- HTTP port change
- CLI Quick Start script
- Auto save Disable
- Telnet (up to four sessions)
- Telnet out — ability to open Telnet sessions from the box
- Domain Name Service (DNS) capability
- 256 port-based VLANs with IVL — VLAN 1 is the default management VLAN
- 802.1Q tagging
- 802.1p traffic class support / remarking
- Advanced QoS (traffic classification, filtering, mark/remarking, metering, shaping)
- Avaya Automatic-QoS
- Single 802.1d Spanning Tree Protocol (STP) on all ports
- Spanning Tree port mode
- Spanning Tree 802.1d compliance mode
- Port mirroring (1–1)
- Multi-Link Trunking (MLT) with up to six trunks and four links per trunk
- MLT enable/disable whole trunk
- IGMP Multicast no flood command enhancements
- IGMPv1/v2 snooping / proxy
- IGMPv3 Snooping/proxy
- MAC address based security with autolearn (BaySecure)

- Sticky MAC
- RADIUS-based security
- TACACS+
- Local password protection
- SNMPv3 security
- SNMP-based network management
- SNMP MIB web page in EDM
- SNMP Trap list web page in EDM
- Extended IP Manager (IPv4 & IPv6)
- IPv6 Management
- IPv6 VLANs (protocol based)
- No Banner & CTRL-Y Skip
- Local console via serial interface
- 802.3x (Flow Control — Gig ports only)
- BootP/TFTP for downloading software and config file
- RMON (RFC1757): per port Statistics, History, Alarm and Events
- ASCII file configuration
- Syslog
- Dual Syslog servers
- ASCII Config Generator (ACG)
- 802.1X EAP (SHSA, MHMA, MHSA, Guest VLAN, Non-EAP & RADIUS MAC)
- 802.1X Enhancement: Dynamic VLAN assignment for NEAP & MHMA
- 802.1X Enhancement: Unicast request, Non-EAP IP Phone support
- 802.1X RFC3576 RADIUS auth extensions - CoA
- 802.1X RFC2866/2869 RADIUS interim accounting updates
- 802.1X NEAP with VLAN names
- 802.1X NEAP last assigned VLAN
- 802.1X NEAP fail-open VLAN
- 802.1X NEAP re-authentication timer
- 802.1X NEAP and Guest VLAN on same port
- RADIUS EAP / NEAP to different servers
- RADIUS Server reachability
- DA Filtering
- Port Naming

- CANA
- SSHv2
- SSH enhancement to support RSA
- Secure FTP (SFTP)
- Auto Detection And Configuration (ADAC) with 802.1AB interaction
- 802.1AB MED (Cisco IP Phones)
- 802.1AB Location TLV
- 802.1AB and ADAC interoperability
- 802.1AB Integration features
- 802.1AB Customization features
- Identify Units (Blink LEDs)
- Cumulative system uptime (hidden command)
- Virtual LACP
- Static Routing with default route
- IP Local and Non-Local static routing
- BootP/DHCP Relay
- Proxy ARP
- UDP forwarding
- DHCP Snooping
- DHCP Client
- DHCP Option 82
- Dynamic ARP Inspection
- IP Source Guard
- BDPU Filtering
- MAC flush
- Software Exception Log
- CPU & Memory Utilization
- Configure Asset ID
- Show environmental
- Show software status

Chapter 3: Introduction

This document provides information you need to configure system monitoring for the Ethernet Routing Switch 3500 Series.

ACLI command modes

Avaya command line interface (ACLI) provides the following configuration modes:

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

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.

Command mode and sample prompt	Entrance commands	Exit commands
User EXEC `3526T>`	No entrance command, default mode.	Type `exit`or `logout`
Privileged EXEC `3526T#`	From User EXEC mode, type: `enable`	Type `exit` or `logout`
Global Configuration `3526T(config)#`	From Privileged EXEC mode, type: `configure`	To return to Privileged EXEC mode, type: `end` or `exit` To exit ACLI completely, type: `logout`
Interface Configuration `3526T(config-if)#`	From Global Configuration mode: To configure a port, type: `interface`	To return to Global Configuration mode, type: `exit`

Command mode and sample prompt	Entrance commands	Exit commands
	`fastethernet <port number>` To configure a VLAN, type: `interface vlan <vlan number>`	To return to Privileged EXEC mode, type: `end` To exit ACLI completely, type: `logout`

For more information about the ACLI configuration modes, see *Avaya Ethernet Routing Switch 3500 Series Fundamentals* (NN47203-102).

Chapter 4: System Monitoring Fundamentals

The Avaya Ethernet Routing Switch 3500 Series provide features that allow you to monitor your network, display switch statistics, log system events, and provide Remote Network Monitoring (RMON).

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), 1minute (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 3500 Series displays diagnostic and operation information though the LEDs on the unit. Familiarize yourself with the interpretation of the LEDs on the 3500 series device. For more information about the interpretation of the LEDs, see *Avaya Ethernet Routing Switch 3500 Series — Quick Install Guide* (NN47203-300).

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 3500 Series Configuration — Security*, (NN47203-504).

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 3500 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).

Software exception log

This feature allows an administrator to see software exceptions generated in the ERS 3500 Series switch. There are three types of software exceptions :

- Data Access exceptions
- Program exceptions
- Watchdog exceptions

These exceptions cause the switch to reset itself. Each time an exception happens, a SYSLOG message is also generated with the severity “Critical” . The message is saved in NVRAM and can be seen using the **show logging** command. NVRAM can store up to 50 Critical/Serious messages. If remote system logging is configured and enabled, the critical message can be sent to a remote server.

You can display and clear the last software exceptions generated in the system using ACLI. See Software exception log using ACLI on page 34.

Note:

After an exception occurs and the switch resets itself, if there is another reset that occurs before the next autosave, then the Critical message in the syslog may be lost.

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 and/or outgoing traffic on the mirrored port is copied to the monitor port. This feature is helpful in network troubleshooting.

You can specify port-based monitoring for ingress and/or egress 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.

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.

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.

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.

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 3500 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.

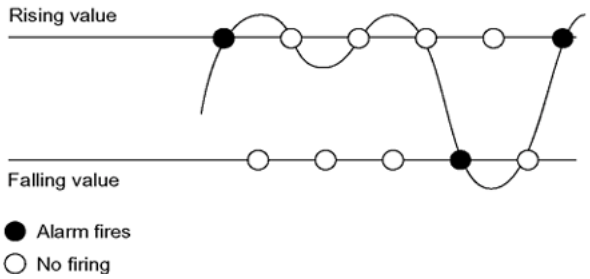

Figure 1: RMON alarm triggers

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.

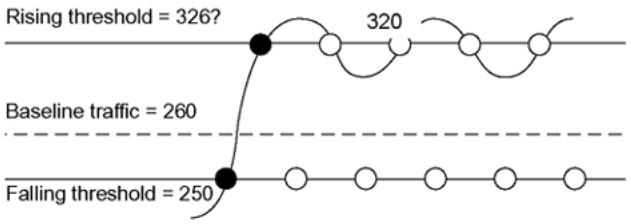

Figure 2: RMON alarm thresholds

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.

Show environmental

The Show Environmental feature provides an enhancement that displays environmental information, in either ACLI or EDM, about the operation of the switch or units within a stack. No specific configuration is required and you do not need to enable or activate this feature.

You can display the following parameters for each switch:

- AC power supply status
- fan status
- system temperature

Note:

AC power supply status information is only available in EDM.

The Show Environmental output depends on the hardware of each unit. For example you can have 2, 3 or 4 fans on one unit, depending on its type. Because the switches have only one primary power supply unit, this is the only one displayed.

The ACLI command is available from any ACLI mode and there are equivalent EDM displays. The following table defines the various states reported by the switch.

Measurement	State	Description
AC power	Normal	If AC or AC/RPSU power is present.
	Unknown	Other unknown state.
Fan	OK	If the fan is working properly.
	FAIL	If any fan malfunction exists.

Measurement	State	Description
	N/A	If the fan does not exist.
Temperature	OK	If the temperature is lower than 50 deg. C.
	HIGH	If the temperature is higher than 50 deg. C.

Dual Syslog Server Support

You can enable dual syslog server support by configuring and enabling a secondary remote syslog server to run in tandem with the first.

The system then sends syslog messages simultaneously to both servers to ensure that syslog messages are recorded, even if one of the servers becomes unavailable.

The servers can use either an IPv4 or IPv6 address.

Chapter 5: Network monitoring configuration using ACLI

Displaying CPU Utilization using ACLI

Display CPU utilization for all units or a specific unit.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   `show cpu-utilization <1–8>`

Variable definitions

The following table describes the parameters for the **`show cpu-utilization`** command.

Variable	Value
<1–8>	Specifies the number of a specific unit.

Displaying Memory Utilization using ACLI

Display memory utilization for all units or a specific unit.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   `show memory-utilization <1–8>`

Variable definitions

The following table describes the parameters for the **show memory-utilization** command.

Variable	Value
<1–8>	Specifies the number of a specific unit

System logs using ACLI

This section describes ACLI command that you use to configure and manage the system logs.

Displaying The System Event Log using ACLI

Display the configuration and the current contents of the system event log.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   `show logging`

Variable definitions

The following table describes the parameters for the **show logging** command.

Variable	Value
config	Specifies the configuration of event logging.
critical	Displays critical log messages.
informational	Displays informational log messages.
serious	Displays serious log messages.
sort-reverse	Displays informational log messages in reverse chronological order (beginning with most recent).

Variable	Value
unit	Specifies the log messages for a certain unit.

Configuring System Logging using ACLI

Configure the system settings for the system event log.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
[no] [default] 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 parameters for the **`logging`** command.

Variable	Value
enable|disable	Enables or disables the event log DEFAULT: Enabled
level critical|serious|informational|none	Specifies the level of logging stored in DRAM.
nv-level critical|serious|none	Specifies the level of logging stored in NVRAM.
remote	Configures remote logging parameters: • Address: configure remote syslog address • Enable: enable remote logging • Level: configure remote logging level
volatile	Configures options for logging to DRAM. • Latch: latch DRAM log after it is full • Overwrite: overwrite DRAM log after it is full

Clearing Log Messages using ACLI

Clear all log messages in DRAM.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   ```
   clear logging [non-volatile] [nv] [volatile]
   ```

Variable definitions

The following table describes the parameters for the **`clear logging`** command.

Variable	Value
non-volatile	Clears log messages from NVRAM.
nv	Clears log messages from NVRAM and DRAM.
volatile	Clears log messages from DRAM.

Configuring Remote System Logging using ACLI

Manage the logging of system messages on a remote server.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   logging remote [address <A.B.C.D | WORD>] [secondary-address
   <A.B.C.D | WORD>] [enable} {level <critical|informational |
   none | serious>] [facility <daemon| local0 | local1 | local2
   | local3 | local4 | local5 | local6 | local7>]
   ```

Variable definitions

The following table describes the parameters for the **`logging remote`** command.

Variable	Value
address <*A.B.C.D* | *WORD*>	Specifies the primary remote system log server IP address. • A.B.C.D is the IPv4 address of the remote server • WORD is the remote host IPv6 address. The value is a character string with a maximum of 45 characters.
enable	Enables system message logging on the remote server. You must configure either the primary or secondary remote server IP address before you can enable remote logging.
facility <*daemon*| *local0* | *local1* | *local2* | *local3* | *local4* | *local5* | *local6* | *local7*>	Specifies remote logging facility.
level<*critical*|*informational*|*none*|*serious*>	Specifies the level of system messages to send to the remote system log server: • critical —only events classified as critical are sent to the remote system log server • serious —only events classified as serious are sent to the remote system log server • informational —only events classified as informational are sent to the remote log server • none —no system log messages are sent to the remote system log server
secondary-address<*A.B.C.D*|<*WORD*>	Specifies the secondary remote system log server IP address: • A.B.C.D. is the IPv4 address of the remote server • WORD is the remote host IPv6 address. The value is a character string with a maximum of 45 characters

Displaying System Logging Information using ACLI

Configures information for system logging.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   `show logging [config] [critical] [informational] [serious] [sort-reverse] [unit <1–8>`

Example

The following figure provides a sample of **`show logging`** command.

```
3524GT-PWR+#show logging
Type Time                          Idx  Src Message
---- ----------------------------- ---- --- -------
S    00:00:00:00                   1    NVR Switch IP changed
S    00:00:00:00                   2    NVR Gateway IP changed
S    00:00:00:00                   3    NVR Download - AGENT image
v5.0.                                          0.38 programmed successfully
S    00:00:00:00                   4    NVR Download - AGENT image
v5.0.                                       0.40 programmed successfully
S    00:00:00:00                   5    NVR Download - AGENT image
v5.0.                                       0.41 programmed successfully
S    00:00:00:00                   6    NVR #1 Reset initiated through
                                        telnet by IP address:
192.168.20                                       1.149, access mode: no security
S    00:00:00:00                   7    NVR Download - AGENT image
v5.0.                                       0.41 programmed successfully
S    00:00:00:00                   8    NVR Download - AGENT image
v5.0.                                       0.41 programmed successfully
I    00:00:00:17                   9    Web server starts service on
                                        port 80.
I    00:00:01:56                   10   Warm Start Trap
I    00:00:01:56                   11   Trap:

lldpXMedTopologyChangeDetected,                                          Subtype = 4
Class = 4
I    00:00:01:56                   12   Trap:lldpRemTableChange Inserts =
----More (q=Quit, space/return=Continue)----
```

Variable definitions

The following table describes the parameters for the **`show logging`** command.

Variable	Value
config	Displays local and remote system logging configuration status

Variable	Value
critical	Displays critical log messages
informational	Displays informational log messages
serious	Displays serious log messages
sort-reverse	Displays informational log messages in reverse chronological order (beginning with most recent)
unit<*1–8*>	Specifies log messages for a specific switch

Disabling Remote System Logging using ACLI

Disable the logging of system messages on a remote server.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   no logging remote [address] [secondary-address] [enable]
   [level] [facility]
   ```

Variable definitions

The following table describes the parameters for the **`no logging remote`** command.

Variable	Value
address	Clears the primary remote system log server IP address
enable	Disables system logging on the remote server
level	Clears the remote server logging level
secondary-address	Clears the secondary remote system log server IP address
Facility	Restores factory default remote logging facility

Variable definitions

The following table describes the parameters for the **`default logging remote`** command.

Variable	Value
address	Restores the primary remote system log server IP address to the factory default DEFAULT: 0.0.0.0
facility	Restores factory default remote logging facility
level	Restores the remote server logging level to the factory default DEFAULT: none
secondary-address	Restores the secondary remote system log server IP address to the factory default DEFAULT: 0.0.0.0

Restoring Remote System Logging using ACLI

Restore to factory default the logging of system messages on a remote server.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   default logging remote [address] [secondary-address] [level] [facility]
   ```

Software exception log using ACLI

This section describes ACLI commands that you use to display and clear software exception logs.

Displaying last generated software exception log using ACLI

Display the last generated software exception log for debugging purposes.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   `show system last-exception`

Note:

This command produces output that is a series of hex values that can only be decoded by a developer. Use the **`show logging`** command to produce readable exception log information.

Example

The following figure provides a sample of the exception log as displayed in NVRAM using the **`show logging`** command.

```
Type  Time          Idx Src Message
------------------------------------
C     00:00:00:06    7  Sw Exception: Task tFault, Type Data Access, PC 0x00c792c4,
SP 0x0675af70
```

Clearing last generated software exception log using ACLI

Erase the last generated software exception log after viewing.

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   `clear system last–exception`

Port Mirroring using ACLI

This section describes the ACLI commands that you use to configure and display port mirroring.

Configuring Port-Mirroring using ACLI

Configure port mirroring.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   port-mirroring mode {disable|Xrx|Xtx|XrxOrXtx} monitor-port
   <portlist> mirror-port-X <portlist>
   ```

Variable definitions

The following table describes the parameters for the **`port-mirroring mode`** command.

Variable	Value
disable	Disables port-mirroring
Xrx	Mirrors packets received on port X
Xtx	Mirrors packets transmitted on port X
XrxOrXtx	Mirrors packets received or transmitted on port X
<portlist>	Specifies the port to be configured

Disabling Port-Mirroring using ACLI

Disable port mirroring.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   no port-mirroring
   ```

Port Statistics using ACLI

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

Displaying Port-Statistics using ACLI

Display port statistics.

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   `show port-statistics [port <portlist>]`

Example

The following figure provides a sample of **`show port-statistics`** command.

```
3524GT-PWR+#show port-statistics port 1
Received
    Packets:                0
    Multicasts:             0
    Broadcasts:             0
    Total Octets:           0
    FCS Errors:             0
    Undersized Packets:     0
    Oversized Packets:      0
    Filtered 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
Packets     64 bytes:       0
            65-127 bytes:   0
            128-255 bytes:  0
            256-511 bytes:  0
            512-1023 bytes: 0
            1024-1518 bytes: 0
            Jumbo:          0
```

```
    Dropped on No Resources: 0
3524GT-PWR+#
```

Variable definitions

The following table describes the parameters for the **show port-statistics** command.

Variable	Value
port<*portlist*>	Specifies the port numbers for which to display statistics. **Important:** If you omit this parameter, the system uses the port number you specified when selecting the interface.

Clearing Statistical Information using ACLI

Clear all statistical information for the specified port and set all counters to zero (0).

Procedure

1. Log on to ACLI in Interface Configuration command mode.
2. At the command prompt, enter the following command:
   `clear-stats [port <portlist>]`

Variable definitions

The following table describes the parameters for the **clear-stats** command.

Variable	Value
port<*portlist*>	Specifies the port number for which to display statistics **Important:** If you omit this parameter, the system uses the port number you specified when selecting the interface.

Configuring LEDs to blink on the Display Panel using ACLI

Set the LEDs on the display panel to blink to identify a particular unit

Procedure

1. Log on to ACLI in Privileged EXEC command mode.
2. At the command prompt, enter the following command:
   `blink-leds [off | time <1–10> | unit <1–8> ]`

Example

The following figure provides a sample of the **`blink-leds`** command.

Variable definitions

The following table describes the parameters for the **`blink-leds`** command.

Variable	Value
[off | time<*1–10*>	Specifies whether the LEDs blink or not [off]. If the LEDs blink, this parameter is set to blink from 1 to 10 times
unit<*1–8*>	Specifies which unit [1 to 8] will blink

Chapter 6: 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 3500 Series.

Displaying CPU and memory utilization using EDM

Use this procedure to view both CPU and memory utilzation.

Procedure

1. In 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.
5. On the toolbar, click **Refresh** to update the data.

CPU Mem Utilization tab field descriptions

The following table describes the fields on the CPU/Mem Utilization tab.

Name	Description
Unit	Displays the numerical representation of the unit
Last10Seconds	Displays CPU usage, in percentage, for the last 10 seconds
Last1Minute	Displays CPU usage, in percentage, for the last minute

Name	Description
Last10minutes	Displays CPU usage, in percentage, for the last 10 minutes
Last1hour	Displays CPU usage, in percentage, for the last hour
Last24Hours	Displays CPU usage, in percentage, for the last 24 hours
TotalCPUUsage	Displays the CPU load in percentage since the boot
MemoryTotalMB	Displays total memory present, in megabytes, on the unit
MemoryAvailableMB	Displays memory remaining available on the unit
MemoryUsedMB	Displays memory that has been used on the unit

Displaying switch power supply information using EDM

Use this procedure to display power supply status for the switch.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Environment**.
4. In the work area, click the **PowerSupply** tab.
5. On the toolbar, click **Refresh** to update the data.

PowerSupply tab field descriptions

The following table describes the fields on the PowerSupply tab.

Name	Description
Unit	Displays the switch.
Power Supply	Displays the power status for the switch.

Displaying switch fan information using EDM

Use this procedure to display information about the operating status of the switch fans.

Procedure

1. In the navigation tree, double-click **Edit** .
2. In the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Environment**.
4. On the work area, click the **Fan** tab.
5. On the toolbar, click **Refresh** to update the information.

Fan tab field descriptions

The following table describes the fields on the Fan tab.

Name	Description
Unit 1 Fan 1	Indicates the status of Fan 1.
Unit 1 Fan 2	Indicates the status of Fan 2.
Unit 1 Fan 3	Indicates the status of Fan 3.
Unit 1 Fan 4	Indicates the status of Fan 4.

Displaying switch temperature using EDM

Use this procedure to display switch temperature information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Environment**.
4. In the work area, click the **Temperature** tab.

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

Temperature tab field descriptions

The following table describes the fields on the Temperature tab.

Name	Description
Unit	Indicates the number of the switch. DEFAULT: 1
Temperature	Indicates the switch unit operating temperature.

Configuring remote system logging using EDM

Use this procedure to configure and manage the logging of system messages.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **System Log**.
4. In the work area, click the **Remote System Log** tab to display the Remote System Log Information.
5. In the **RemoteSyslogAddressType** field, choose the type of IP address for the primary remote system log server.
6. In the **RemoteSyslogAddress** box, enter the IP address for the primary remote system log server.
7. OPTIONAL: In the **SecondarySyslogAddressType** field, choose the type of IP address for the secondary remote system log server.
8. OPTIONAL: In the **SecondarySyslogAddress** box, enter the IP address for the secondary remote system log server.
9. Do one of the following:
   - Select the **Enabled** check box to enable remote system logging.
   - Clear the **Enabled** check box to disable remote system logging.

10. In the **Save Targets** box, select the types of messages you want the system to report to the remote system log server or servers (if you are using Dual Syslog Servers).
11. In the **Facility** box, specify the remote logging facility.
12. On the toolbar, click **Apply**.

Remote System Log tab field descriptions

The following table describes the fields on the Remote System Log tab.

Name	Description
RemoteSyslogAddressType	Specifies the type of IP address for the remote system log server.
RemoteSyslogAddress	Specifies the IP address for the remote system log server to send system log messages to.
SecondarySyslogAddressType	Specifies the type of IP address for the secondary remote system log server.
SecondarySyslogAddress	Specifies the IP address for the secondary remote system log server to send system log messages to.
Enabled	Specifies whether or not remote logging is enabled.
Save Targets	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**: only messages classified as critical are sent to the remote system log server • **critical/serious**: only messages classified as critical and serious are sent to the remote system log server. • **critical/serious/inform**: only messages classified as critical, serious, and informational are sent to the remote system log server. • **none**: no system log messages are sent to the remote system log server.

Name	Description
Facility	Specifies the type of remote logging facility as one of the following: • Daemon • Local0 • Local1 • Local2 • Local3 • Local4 • Local5 • Local6 • Local7

Displaying system log settings using EDM

Use this procedure to view System Log Settings information.

Procedure

1. In 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.

System Log Settings tab field descriptions

The following table describes the fields on the System Log Settings tab.

Name	Description
Operation	Enables you 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

Name	Description
	specify **off,** the system discontinues log message accumulation. **Important:** This does not affect operation of the remote syslog facility; it only determines whether log messages are stored locally.
BufferFullAction	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).
Volatile —CurSize	Displays the current number of log messages in the volatile portion of the system log messages facility. Messages that are classified as volatile are lost upon system reinitialization.
Volatile —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 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 in the system. 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.
non-Volatile —CurSize	Displays the current number of log messages that are present in the nonvolatile portion of the system log message facility.

Name	Description
	Messages that are classified as nonvolatile are saved across system reinitilizations.
non-Volatile —SaveTargets	Determines the type of log messages that are saved to nonvolatile storage after they occur. Messages are classified based on their type as follows: • critical • critical/serious • none 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 in the system. 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.
Action — ClearMessageBuffers	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 bits are deleted. For example, specifying volInformational deletes all informational messages and specifying nonVolCritical deletes all critical messages from nonvolatile storage.

Displaying system logs using EDM

Use this procedure to view System Logs information.

Procedure

1. In 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.

System Logs tab field descriptions

The following table describes the fields on the System Logs tab.

Name	Description
OrigUnitNumber	Specifies the unit number of the originator of the log message.
MsgTime	Specifies the time (in hundredths of a second) between system initialization and the time this log message was entered into the system.
MsgIndex	Specifies the arbitrary integer index assigned to the log message upon entry into the message facility.
MsgSrc	Specifies the message source that indicates whether this message is loaded from nonvolatile storage at system initialization or whether the message is generated after that time.
MsgString	Specifies a printable string indicating the originator of and the reason why a log message is generated. This string, coupled with the log message parameters that are associated with the message, provides an understanding of the log message.
MsgType	Specifies the type of system message.

Displaying network topology information using EDM

Use this procedure to display network topology information.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics work area, click the **Topology** tab.

4. In the Status section, configure as required.
5. On the toolbar, click **Apply**.

Variable definitions

The following table describes the variables associated with displaying network topology information.

Name	Description
IpAddr	Indicates the IP address of the device.
Status	Specifies whether Avaya topology is on (topOn) or off (topOff) for the device. DEFAULT: topOn
NmmLstChg	Indicates the value of sysUpTime the last time an entry in the network management MIB (NMM) topology table was added, deleted, or modified. If the table has not changed since the last cold or warm start of the agent.
NmmMaxNum	Indicates the maximum number of entries in the NMM topology table.
NmmCurNum	Indicates the current number of entries in the NMM topology table.

Displaying the topology table using EDM

Use this procedure to display the topology table.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics work area, click the **Topology** tab.
4. In the Topology section, click the **Topology Table** tab.

Variable definitions

The following table describes the variables associated with displaying the topology table.

Variable	Value
Slot	Indicates the slot number in the chassis in which the topology message was received.
Port	Indicates the port on which the topology message was received.
IpAddr	Indicates the IP address of the sender of the topology message.
SegId	Indicates the segment identifier of the segment from which the remote agent sent the topology message. This value is extracted from the message.
MacAddr	Indicates the MAC address of the sender of the topology message.
ChassisType	Indicates the chassis type of the device that sent the topology message.
BkplType	Indicates the backplane type of the device that sent the topology message.
LocalSeg	Indicates if the sender of the topology message is on the same Ethernet segment as the reporting agent.
CurState	Indicates the current state of the sender of the topology message. The choices are: • topChanged — Topology information has recently changed. • heartbeat — Topology information is unchanged. • new — The sending agent is in a new state.

Port Mirroring using EDM

This section provides procedures to display and configure the Port Mirroring feature using EDM.

Displaying Port Mirroring using EDM

Use this procedure to troubleshoot the network.

Procedure

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

Port Mirrors tab field descriptions

The following table describes the fields on the Port Mirrors tab.

Name	Description
Instance	Indicates the Port Mirroring instance number. Release 5.0 supports only 1 instance.
PortMode	Indicates the supported Port Mirroring modes. The modes are: • **Xrx**— monitors all traffic received on port **X**. • **XrxOrXtx**— monitors all traffic received or transmitted on port **X**. • **Xtx** — monitors all traffic transmitted on port **X**.
MonitorPort	Indicates the switch port to designate as the monitor port.
PortListX	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.

Configuring Port Mirroring using EDM

Use this procedure to help you troubleshoot the network.

Procedure

1. In 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**.

Port Mirrors tab field descriptions

The following table describes the fields on the Port Mirrors tab.

Name	Description
Instance	Specifies the Port Mirroring instance number. Release 5.0 supports only 1 instance.
PortMode	Specifies the supported Port Mirroring modes. The modes are: • **Xrx**— monitors all traffic received on port **X**. • **XrxOrXtx**— monitors all traffic received or transmitted on port **X**. • **Xtx** — monitors all traffic transmitted on port **X**.
MonitorPort	Specifies the switch port to designate as the monitor port.

Name	Description
PortListX	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.

Graphing chassis statistics using EDM

Use this procedure to graph chassis statistics.

Procedure

1. In 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.

Displaying IP statistics using EDM

Use this procedure to view and graph IP statistics.

Procedure

1. In 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.

IPtab field descriptions

The following table describes the fields on the IPtab.

Name	Description
InReceives	Specifies the total number of input datagrams received from interfaces, including those received in error.
InHdrErrors	Specifies 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.
InAddrErrors	Specifies 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 do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ForwDatagrams	Specifies 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.
InUnknownProtos	Specifies the number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InDiscards	Specifies 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

Name	Description
	datagrams discarded while awaiting reassembly.
InDelivers	Specifies the total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	Specifies 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.
OutDiscards	Specifies 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.
OutNoRoutes	Specifies 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.
FragOKs	Specifies the number of IP datagrams successfully fragmented at this entity.
FragFails	Specifies 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.
FragCreates	Specifies the number of generated IP datagram fragments because of a fragmentation at this entity.
ReasmReqds	Specifies the number of IP fragments received that needed to be reassembled at this entity.
ReasmOKs	Specifies the number of IP datagrams successfully reassembled.
ReasmFails	Specifies the number of failures detected by the IP reassembly algorithm (for example,

Name	Description
	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.

Displaying ICMP In statistics using EDM

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

Procedure

1. In 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 the 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.

ICMP Intab field descriptions

The following table describes the fields on the ICMP In tab.

Name	Description
SrcQuenchs	Displays the number of ICMP Source Quench messages received.
Redirects	Displays the number of ICMP Redirect messages received.
Echos	Displays the number of ICMP Echo (request) messages received.
EchoReps	Displays the number of ICMP Echo Reply messages received.
Timestamps	Displays the number of ICMP Timestamp (request) messages received.

Name	Description
TimestampReps	Displays the number of ICMP Timestamp Reply messages received.
AddrMasks	Displays the number of ICMP Address Mask Request messages received.
AddrMaskReps	Displays the number of ICMP Address Mask Reply messages received.
ParmProbs	Displays the number of ICMP Parameter Problem messages received.
DestUnreachs	Displays the number of ICMP Destination Unreachable messages received.
TimeExcds	Displays the number of ICMP Time Exceeded messages received.

Displaying ICMP Out statistics using EDM

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

Procedure

1. In 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 the 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.

ICMP Out tab field descriptions

The following table describes the fields on the ICMP Out tab.

Name	Description
SrcQuenchs	Displays the number of ICMP Source Quench messages sent.
Redirects	Displays the number of ICMP Redirect messages received. For a host, this object is

Name	Description
	always zero because hosts do not send redirects.
Echos	Displays the number of ICMP Echo (request) messages sent.
EchoReps	Displays the number of ICMP Echo Reply messages sent.
Timestamps	Displays the number of ICMP Timestamp (request) messages sent.
TimestampReps	Displays the number of ICMP Timestamp Reply messages sent.
AddrMasks	Displays the number of ICMP Address Mask Request messages sent.
AddrMaskReps	Displays the number of ICMP Address Mask Reply messages sent.
ParmProbs	Displays the number of ICMP Parameter Problem messages sent.
DestUnreachs	Displays the number of ICMP Destination Unreachable messages sent.
TimeExcds	Displays the number of ICMP Time Exceeded messages sent.

Displaying TCP statistics using EDM

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

Procedure

1. In 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 the 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.

TCP tab field descriptions

The following table describes the fields on the TCP tab.

Name	Description
ActiveOpens	Displays the number of times TCP connections make a direct transition to the SYN-SENT state from the CLOSED state.
PassiveOpens	Displays the number of times TCP connections make a direct transition to the SYN-RCVD state from the LISTEN state.
AttemptFails	Displays 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 SYNRCVD state.
EstabResets	Displays the number of times TCP connections make a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
CurrEstab	Displays the number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
InSegs	Displays the total number of segments received, including those received in error. This count includes segments received on currently established connections.
OutSegs	Displays the total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
ReTransSegs	Displays the total number of segments retransmitted, that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
InErrs	Displays the total number of segments received in error (for example, bad TCP checksums).
OutRsts	Displays the number of TCP segments sent containing the RST flag.

Name	Description
HcInSegs	Displays the number of segments received, including those received in error. This count includes segments received on currently established connections. This object is the 64-bit equivalent of InSegs.
HCOutSegs	Displays the number of segments sent, including those on current connections, but excluding those containing only retransmitted octets. This object is the 64-bit equivalent of OutSegs.

Displaying UDP statistics using EDM

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

Procedure

1. In 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 the 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.

UDP tab field descriptions

The following table describes the fields on the UDP tab.

Name	Description
InDatagrams	Displays the total number of UDP datagrams delivered to UDP users.
NoPorts	Displays the total number of received UDP datagrams for which there was no application at the destination port.
InErrors	Displays the number of received UDP datagrams that cannot be delivered for

Name	Description
	reasons other than the lack of an application at the destination port.
OutDatagrams	Displays the total number of UDP datagrams sent from this entity.
HCInDatagrams	Displays the number of TCP connections for which the current state is either **ESTABLISHED or CLOSE-WAIT**.
HCOutDatagrams	Displays 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.

Displaying 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

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

Procedure

1. On the Device Physical View, click on the port you want to graph.
2. In 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

Use this procedure to display and graph interface parameters for a port.

Procedure

1. On the Device Physical View, click on a port.
2. In 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.

Interface tab field descriptions

The following table describes the fields on the Interface tab.

Name	Description
InOctets	Displays the total number of octets received on the interface, including framing characters.
OutOctets	Displays the total number of octets transmitted out of the interface, including framing characters.
InUcastPkts	Displays 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.
OutNUcastPkts	Displays 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.

Name	Description
InMulticastPkts	Displays 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.
OutMulticastPkts	Displays 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.
InBroadcastPkts	Displays the number of packets delivered by this sublayer to a higher sublayer that are addressed to a broadcast address at this sublayer.
OutBroadcastPkts	Displays 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.
InDiscards	Displays 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.
OutDiscards	Displays the number of outbound packets chosen to be discarded even though no errors were detected to prevent them from being transmitted. One possible reason for discarding such a packet can be to free up buffer space.
InErrors	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.
OutErrors	For packet-oriented interfaces, the number of outbound packets that cannot be transmitted because of errors. For character-

Name	Description
	oriented or fixed-length interfaces, the number of outbound transmission units that cannot be transmitted because of errors.
InUnknownProtos	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.

Graphing Ethernet error statistics using EDM

Use this procedure to view and graph Ethernet error statistics.

Procedure

1. On the Device Physical View, click on a port.
2. In 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.

Ethernet Errors tab field descriptions

The following table describes the fields on the Ethernet Errors tab.

Name	Description
AlignmentErrors	Specifies a count of frames received on a particular interface that are not an integral number of octets in length and do not pass

Name	Description
	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.
FCSErrors	Specifies 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.
InternalMacTransmitErrors	Specifies 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.
InternalMacReceiveErrors	Specifies 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.
CarrierSenseErrors	Specifies a number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a

Name	Description
	particular interface. The count represented by an instance of this object is incremented at most once for each transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
FrameToolLongs	Specifies 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.
SQETestErrors	Specifies 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.
DeferredTransmissions	Specifies 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.
SingleCollisionFrames	Specifies 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.
MultipleCollisionFrames	Specifies 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

Name	Description
	ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	Specifies 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.
ExcessiveCollisions	Specifies a count of frames for which transmission on a particular interface fails due to excessive collisions.

Graphing miscellaneous statistics using EDM

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

Procedure

1. On the Device Physical View, click on a port.
2. In 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.

Misc. Stats tab field descriptions

The following table describes the fields on the Misc. Stats tab.

Name	Description
NoResourcesPktsDropped	Displays the number of packets dropped due to switch memory shortage.

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

Use this procedure to view the response of an SNMP Get and Get-Next request for any Object Identifier (OID) on the EDM Management Information Base (MIB) Web page.

Procedure

1. In 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

Use this procedure to retrieve a subtree of the MIB that has the SNMP object as root and request the result of MIB Walk.

Procedure

1. In 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 of the window. If the request is unsuccessful, a description of the received error appears.

Chapter 7: RMON using ACLI

Displaying RMON Alarms using ACLI

Displays information about RMON alarms.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   `show rmon alarm`

Displaying the RMON Events using ACLI

Displays information about RMON events.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   `show rmon event`

Displaying RMON History using ACLI

Displays information about RMON events

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
show rmon history
```

Displaying RMON Statistics using ACLI

Displays information about the configuration of RMON statistics

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   show rmon stats
   ```

Displaying RMON History for a Port using ACLI

Displays RMON history for a port.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   show rmon ethernet history port [LINE]
   ```

Variable definitions

The following table describes the parameters for the **`show rmon ethernet history port`** command.

Variable	Value
LINE	Specifies a list of ports

Displaying RMON Packets for a Port using ACLI

Display RMON packets for all ports or specific ports.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   `show rmon ethernet packets [port <LINE>]`

Variable definitions

The following table describes the parameters for the **`show rmon ethernet packets port`** command.

Variable	Value
LINE	Specifies a list of ports

Displaying RMON Statistics for a Port using ACLI

Displays RMON statistics for all or specific ports..

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   `show rmon ethernet statistics [port <LINE>]`

Variable definitions

The following table describes the parameters for the **show rmon ethernet statistics port** command.

Variable	Value
LINE	Specifies a list of ports

Configuring RMON Alarms using ACLI

Set RMON alarms and thresholds.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
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 the **rmon alarm** command.

Variable	Value
<1–65535>	Specifies the unique index for the alarm entry
<WORD>	Specifies the MIB object to be monitored. This is an object identifier, and for most available objects, an English name can be used
<1–2147483647>	Specifies the sampling interval, in seconds
absolute	Specifies absolute values (value of the MIB object is compared directly with thresholds)

Variable	Value
delta	Specifies delta values (change in the value of the MIB object between samples is compared with thresholds)
rising-threshold<*-2147483648–2147483647 > [<1–65535>]*	Specifies 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
falling-threshold<*-2147483648–2147483647 > [<1–65535>]*	Specifies 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.
[owner <LINE>]	Specifies the owner string to identify the alarm entry

Deleting RMON Alarms using ACLI

To delete RMON alarm table entries.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   `no rmon alarm [<1–65535>]`

Variable definitions

The following table describes the parameters for the **`no rmon alarm`** command.

Variable	Value
<1–65535>	Specifies the unique identifier of the alarm. When the variable is omitted, all entries in the table are cleared

Configuring RMON Events Settings using ACLI

Configure RMON event log and trap settings.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   [no] rmon event <1–65535> [log] [trap] [description <LINE>]
   [owner <LINE>]
   ```

Variable definitions

The following table describes the parameters for the **`rmon event`** command.

Variable	Value
[no]	Deletes RMON event table entries. When the variable *<1–65535>* is omitted, all entries in the table are cleared.
<1–65535>	Specifies the unique index for the event entry
[log]	Records events in the log table
[trap]	Generates SNMP trap messages for events
[description]*<LINE>*	Specifies a textual description for the event
[owner]*<LINE>*	Specifies the owner string to identify the event entry

Configuring RMON History Settings using ACLI

Configure RMON history settings

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:

```
[no] rmon history <1–65535> <LINE> <1–65535> <1–3600> [owner
<LINE>]
```

Variable definitions

The following table describes the parameters for the **`rmon history`** command.

Variable	Value
[no]	Deletes RMON history table entries
<*1–65535*>	Specifies the unique index for the history entry
<*LINE*>	Specifies the port number to be monitored
<*1–65535*>	Specifies the number of history buckets (records) to keep.
<*1–3600*>	Specifies the sampling rate (how often a history sample is collected).
[owner]<*LINE*>	Specifies the owner string to identify the history event

Configuring RMON Statistics Settings using ACLI

Configure RMON statistics settings

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   [no] rmon stats <1–65535> <LINE> [owner <LINE>]
   ```

Variable definitions

The following table describes the parameters for the **rmon stats** command.

Variable	Value
[no]	Disable RMON statistics. When the variable is omitted, all entries in the table are cleared
<1–65535>	Specifies the unique index for the stats entry
[owner]*<LINE>*	Specifies the owner string to identify the stats entry

Displaying Environmental Status using ACLI

View the Environmental status of the switch.

Procedure

1. Log on to ACLI in User EXEC command mode.
2. At the command prompt, enter the following command:
   `show environmental`

Note:

You can use the command from Global Configuration mode or User EXEC mode.

Example

The following figure provides a sample of **show environmental** command.

```
3510GT-PWR+#show environmental
Unit# FAN1 FAN2 FAN3 FAN4 Temperature
----- ---- ---- ---- ---- -----------
1     OK   N/A  N/A  N/A   OK   39.5C
3510GT-PWR+#
```

Chapter 8: RMON using Enterprise Device Manager

The Remote Network Monitoring (RMON) MIB is an interface between the RMON agent on an Ethernet Routing Switch 3500 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

Working with RMON information:

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

Displaying RMON statistics using EDM

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.

The following types of RMON statistics are available:

- Absolute — The total count since the last time counters were reset. A system restart resets all counters
- Cumulative — 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.
- Average/sec — The cumulative count divided by the cumulative elapsed time.
- Min/sec — The minimum average for the counter for a given polling interval over the cumulative elapsed time.

- Max/sec — The maximum average for the counter for a given polling interval over the cumulative elapsed time.
- Last/Val/sec — The average for the counter over the last polling interval.

Perform this procedure to view RMON Ethernet statistics.

Procedure

1. On the Device Physical View, lick on a port.
2. In the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **RMON** tab.
5. Click the 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.

RMON tab field descriptions

The following table describes the fields on the RMON tab.

Name	Description
Octets	Displays 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.
Pkts	Displays the total number of packets (including bad packets, broadcast packets, and multicast packets) received.
BroadcastPkts	Displays the total number of good packets received that are directed to the broadcast address. This does not include multicast packets.
MulticastPkts	Displays the total number of good packets received that are directed to a multicast

Name	Description
	address. This number does not include packets directed to the broadcast address.
CRCAlignErrors	Displays 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).
UndersizePkts	Displays 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.
Fragments	Displays 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.
Collisions	Displays the best estimate of the total number of collisions on this Ethernet segment.
Jabbers	Displays 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.
1 to 64	Displays 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).
65 to 127	Displays the total number of packets (including bad packets) received that are greater than 64 octets in length (excluding framing bits but including FCS octets).

Name	Description
128 to 255	Displays the total number of packets (including bad packets) received that are greater than 127 octets in length (excluding framing bits but including FCS octets).
256 to 511	Displays the total number of packets (including bad packets) received that are greater than 255 octets in length (excluding framing bits but including FCS octets).
512 to 1023	Displays the total number of packets (including bad packets) received that are greater than 511 octets in length (excluding framing bits but including FCS octets).
1024 to 1518	Displays the total number of packets (including bad packets) received that are greater than 1023 octets in length (excluding framing bits but including FCS octets).
OversizePkts (>1518)	Displays the total number of packets received that are longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.

Configuring the IPv4 remote access list using EDM

Use this procedure to configure a list of IPv4 source addresses for which to permit remote access to a switch.

Procedure

1. From the navigation tree, double-click **Administration**.
2. In the Administration tree, click **Remote Access**.
3. In the Remote Access work area, click the **Allowed List(IPv4)** tab.
4. In the Allowed List (IPv4) section, configure as required.
5. On the toolbar, click **Apply**.

Variable definitions

The following table describes the variables associated with configuring IPv4 remote access.

Variable	Value
Allowed Source IP Address	Specifies the source IPv4 address to permit remote access to the switch.
Allowed Source Mask	Specifies subnet mask associated with the source IPv4 address to permit remote access to the switch.

Configuring the IPv6 remote access list using EDM

Use this procedure to configure a list of IPv6 source addresses for which to permit remote access to a switch.

Procedure

1. From the navigation tree, double-click **Administration**.
2. In the Administration tree, click **Remote Access**.
3. In the Remote Access work area, click the **Allowed List (IPv6)** tab.
4. In the Allowed List (IPv6) section, configure as required.
5. On the toolbar, click **Apply**.

Variable definitions

The following table describes the variables associated with configuring IPv6 remote access.

Variable	Value
Allowed Source IPv6 Address	Specifies the source IPv6 address to permit remote access to the switch.
Allowed Prefix Length	Specifies prefix length for the source IPv6 address to permit remote access to the switch. RANGE: 0–128.

RMON history management using EDM

Use the following procedures to manage RMON history.

Displaying RMON history using EDM

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–second and 30–minute intervals.
- Number of buckets gather is 15 for the 30–second intervals, and 5 for the 30–minute 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.

Use this procedure to view RMON history.

Procedure

1. In 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 using EDM

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.

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

Before you begin

Procedure

1. In 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, buckets, and interval that you specified.

RMON History tab field descriptions

The following table describes the fields on the RMON History tab.

Name	Description
Index	Specifies a unique value assigned to each interface. An index identifies an entry in a table.
Port	Specifies any Ethernet interface on the device.
BucketsRequested	Specifies 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.
BucketsGranted	Specifies 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

Name	Description
	end of each sampling interval, a new bucket is added to the media-specific table.
Interval	Specifies 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.
Owner	Specifies the network management system that created this entry.

Disabling RMON history using EDM

Use this procedure to disable RMON history on a port.

Procedure

1. In 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 using EDM

Use this procedure to display and graph RMON History statistics.

Procedure

1. In 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**.

Display History Data tab field descriptions

The following table describes the fields on the Display History Data tab.

Name	Description
SampleIndex	Displays 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.
Utilization	Displays the best estimate of the mean physical layer network utilization on this interface during the sampling interval (in hundredths of a percent).
Octets	Displays 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.
Pkts	Displays the total number of packets (including bad packets, broadcast packets, and multicast packets) received.
BroadcastPkts	Displays the total number of good packets received that are directed to the broadcast

Name	Description
	address. This does not include multicast packets.
MulticastPkts	Displays 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.
DropEvents	Displays 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.
CRCAlignErrors	Displays 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).
UndersizePkts	Displays 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.
OversizePkts	Displays the total number of packets received that are longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
Fragments	Displays 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 number of octets (FCS Error), or a nonintegral number of octets (Alignment Error).
Collisions	Displays the best estimate of the number of collisions on an Ethernet segment during a sampling interval.

Ethernet statistics gathering using EDM

Use the following procedures to gather ethernet statistics using EDM.

Enabling Ethernet statistics gathering using EDM

Use this procedure to use RMON to gather Ethernet statistics.

Procedure

1. In 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 of click the ellipsis (...) 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 ellipsis (...) to select a port from the list.
7. In the **Owner** box, type the owner information.
8. Click **Insert**.

Ether Stats tab field descriptions

The following table describes the fields on the Ether Stats tab.

Name	Description
Index	Specifies a unique value assigned to each interface. An index identifies an entry in a table.
Port	Specifies any Ethernet interface on the device.
Owner	Specifies the network management system which created this entity.

Disabling Ethernet statistics gathering using EDM

Use this procedure to disable Ethernet statistics that you have set.

Procedure

1. In 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.

RMON alarm management using EDM

Use the following procedures to manage RMON alarms.

Creating an alarm using EDM

Use this procedure to create an alarm to received statistics and history using default values.

Procedure

1. In 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.

Alarms tab field descriptions

The following table describes the fields on the Alarms tab.

Name	Description
Variable	Specifies the Name and Type of alarm in one of the following formats: • **alarm.x**: where x=0 to indicate a chassis alarm • **alarmname.**: where you specify the index. The index is a card number for module-related alarms, OR 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 the display of the port selection tool.
Sample Type	Specifies either absolute or delta
Interval	Specifies the time period (in seconds) over which the data is sampled and compared with the rising and falling thresholds.
Index	Uniquely identifies an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device.
Rising Threshold	Specifies that 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.
RisingEventIndex	Specifies the 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.)
Falling Threshold	Specifies that when the current sampled value is less than or equal to this threshold, and the value at the last sampling interval

Name	Description
	was greater than this threshold, the alarm generates a single event.
FallingEventIndex	Specifies the 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.)
Owner	Identifies the network management system which created this entry.

Deleting an alarm using EDM

Use this procedure to delete an alarm.

Procedure

1. In 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.

Displaying an event using EDM

Use this procedure to view a table of events.

Procedure

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

Events tab field descriptions

The following table describes the fields on the Events tab.

Name	Description
Index	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.
Description	Specifies whether the event is a rising or falling event.
Type	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: • none • log • 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 set to the owner, this field specifies the name of the machine that receives alarm traps.

Creating an event using EDM

Use this procedure to create an event.

Procedure

1. In 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.
   To designate the event type to
   - save memory — specify the event type as **log**
   - reduce traffic from the switch or improve CPU utilization — 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 using EDM

Use this procedure to delete an event.

Procedure

1. In 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.

Displaying RMON log information using EDM

Use this procedure to open and view information in the **Log** tab.

Procedure

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

Log tab field descriptions

The following table describes the fields on the Log tab.

Name	Description
Time	Displays the value of sysUpTime after this log entry was created.
Description	Displays an implementation-dependent description of the event that activated the log entry.
EventIndex	Displays the index of the event entry.