Configuring System Monitoring on Avaya Ethernet Routing Switch 5000 Series

Release 6.6
NN47200-505
Issue 08.01
December 2013

© 2013 Avaya Inc.

All Rights Reserved.

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 may generally make available to users of its products and Hosted Services. 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 Avaya hardware and software. 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 or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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.

Licence types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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”, or such successor site as designated by Avaya. 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, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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 or Hosted Service 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”). As required, 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 or such successor site as designated by Avaya. 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 or such successor site as designated by Avaya. 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, Hosted Service(s), and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Comments? infodev@avaya.com

Contents

Chapter 1: Introduction 11
- Purpose 11
- Related resources 11
- Support 12

Chapter 2: New in this release 13
- Features 13
  - Remote Switch Port Analyzer (RSPAN) 13
  - Show TCP Ports 13
  - SLA Monitor 13
- Other changes 14
  - CLI interface change from FastEthernet to Ethernet 14

Chapter 3: System monitoring fundamentals 15
- System logging 15
- Remote logging 15
  - Dual syslog server support 16
- Alarms 16
- How RMON alarms work 16
- Creating alarms 18
- Trap Web page 18
- Management Information Base Web page 19
- IGMP and the system event log 19
- Port mirroring 21
  - Port-based mirroring configuration 21
  - Address-based mirroring configuration 22
  - Bi-directional Monitor Port 23
- Many-to-Many Port Mirroring 23
  - Port-based modes 24
  - MAC address-based modes 24
  - Many-to-many port mirroring functionality 24
  - Many-to-many port mirroring restrictions 25
- Remote Switch Port Analyzer (RSPAN) 25
- Stack loopback tests 28
- Stack monitor 29
- CPU and memory utilization 29
- Light Emitting Diode display 30
- Power over Ethernet allocations 30
  - Displaying PoE allocations using ACLI 30
  - Displaying PoE allocations using EDM 31
- IP Flow Information Export 31
- Remote Network Monitoring 32
- Debug trace commands 32
- Stack Health Check 33
- Displaying environmental information 33
- SLA Monitor 33

Chapter 4: System diagnostics and statistics using ACLI 37
Trace diagnosis of problems 37
Trace diagnosis of problems navigation 37
Using trace to diagnose problems 37
Viewing the trace level 39
Viewing the trace module ID list 39
Port statistics 40
Viewing port-statistics 40
Configuring Stack Monitor 40
Viewing the stack-monitor 41
Configuring the stack-monitor 41
Setting default stack-monitor values 42
Disabling the stack monitor 42
Viewing Stack Port Counters 42
Job aid 43
Clearing stack port counters 44
Using the stack loopback test 44
Job aid 45
Displaying port operational status 46
Validating port operational status 46
Showing port information 46
Job aid 47
Showing stack health information 48
Job aid 48
Job aid 50
Displaying the agent and image software load status using ACLI 51
Viewing environmental information 52
Job aid 52
Job aid 52
Displaying TCP ports 53
Chapter 5: Network monitoring configuration using ACLI 55
Viewing CPU utilization 55
Viewing memory utilization 55
Configuring the system log 55
Displaying the system log 56
Configuring the system log 56
Disabling the system log 57
Setting the system log to default 57
Clearing the system log 57
Remote system logging configuration using the ACLI 58
Configuring remote system logging 58
Disabling remote system logging 60
Restoring remote system logging to default 61
Configuring port mirroring 61
Displaying the port-mirroring configuration 61
Configuring port-mirroring 62
Disabling port-mirroring 63

Displaying Many-to-Many port-mirroring 64
Configuring Many-to-Many port-mirroring 64
Disabling Many-to-Many port-mirroring 65
Displaying RSPAN information 66
Configuring Remote Switch Port Analyzer (RSPAN) 67
Chapter 6: RMON configuration using ACLI 69
Configuring RMON with the ACLI 69
Viewing RMON alarms 69
Viewing RMON events 69
Viewing RMON history 69
Viewing RMON statistics 70
Setting RMON alarms 70
Deleting RMON alarm table entries 71
Configuring RMON event log and traps 72
Deleting RMON event table entries 72
Configuring RMON history 73
Deleting RMON history table entries 73
Configuring RMON statistics 74
Disabling RMON statistics 74
Chapter 7: IPFIX Configuration using ACLI 77
Configuring IPFIX collectors 77
Enabling IPFIX globally 78
Configuring unit specific IPFIX 78
Enabling IPFIX on the interface 79
Enabling IPFIX export through ports 79
Deleting the IPFIX information for a port 79
Viewing the IPFIX table 80
Chapter 8: System diagnostics and statistics using Enterprise Device Manager 83
Configuring Stack Monitor using EDM 83
Viewing stack health using EDM 84
Viewing power supply information 84
Viewing switch fan information 85
Viewing switch temperature 86
Chapter 9: Network monitoring configuration using Enterprise Device Manager 89
CPU and memory utilization using EDM 89
Switch stack information management 90
Viewing stack information 90
Editing stack information 92
Viewing pluggable ports 95
Configuring the system log using EDM 96
Viewing system logs using EDM 97
Viewing system log settings 98
Remote system logging using EDM 99
Viewing remote system log properties 100
Configuring remote system logging using EDM 101
EDM MIB Web page 103
Using the EDM MIB Web page for SNMP Get and Get-Next 103

Using the EDM MIB Web page for SNMP walk ... 103
Port Mirroring using EDM ... 104
Viewing Port Mirroring using EDM ... 104
Configuring Port Mirroring using EDM ... 105
Configuring RSPAN ... 107
Creating a graph using EDM ... 108
Graphing switch chassis data using EDM ... 108
Graphing the SNMP tab using EDM ... 109
Graphing the IP tab using EDM ... 111
Graphing the ICMP In tab using EDM ... 112
Graphing the ICMP Out tab using EDM ... 113
Graphing the TCP tab using EDM ... 114
Graphing the UDP tab using EDM ... 116
Graphing switch port data using EDM ... 117
Graphing the Interface tab using EDM ... 117
Graphing Ethernet Errors tab using EDM ... 119
Graphing the Bridge tab using EDM ... 121
Graphing the Rmon tab using EDM ... 122
Graphing the EAPOL Stats tab using EDM ... 124
Viewing and graphing the EAPOL Diag tab using EDM ... 125
Graphing the LACP tab using EDM ... 128
Graphing the Misc tab ... 129
Graphing multilink trunk statistics using EDM ... 130
Accessing MLT statistics window ... 130
Viewing the Interface tab using EDM ... 130
Viewing the Ethernet Errors tab using EDM ... 132
Graphing VLAN DHCP statistics using EDM ... 135
Viewing unit statistics using EDM ... 135
Chapter 10: RMON configuration using Enterprise Device Manager ... 137
Working with RMON information using EDM ... 137
Viewing statistics using EDM ... 137
Viewing history using EDM ... 140
Viewing RMON history statistics using EDM ... 142
Enabling ethernet statistics gathering using EDM ... 144
Configuring Alarm Manager using EDM ... 145
Creating an Alarm using EDM ... 145
Deleting an alarm using EDM ... 146
Configuring Events using EDM ... 149
How events work ... 149
Viewing an event using EDM ... 149
Creating an event using EDM ... 150
Deleting an event using EDM ... 151
Viewing log information using EDM ... 152
Chapter 11: IPFIX configuration using Enterprise Device Manager ... 153
Configuring Global IPFIX ... 153
Configuring IPFIX flows ... 153
Configuring IPFIX collectors ... 155

Creating a collector using EDM 155
Modifying collectors 156
Deleting a collector 157
Configuring IPFIX ports 157
Displaying IPFIX data information 158
Graphing Exporter Statistics using EDM 160
Viewing the IPFIX collector clear time 160
Chapter 12: Topology configuration using Enterprise Device Manager 163
Viewing topology information 163
Viewing topology table information 164
Chapter 13: Configuring the SLA Monitor using ACLI 165
Displaying SLA Monitor agent settings 165
Configuring SLA Monitor using ACLI 166
Executing a new trace route test 171
Executing a real time protocol test 172
Chapter 14: Configuring the SLA Monitor using EDM 175
Configuring SLA Monitor 175
Viewing NTR test results 179
Viewing NTR per-hop test data 181
Executing RTP tests using EDM 182
Viewing RTP results 183
Index 187

Chapter 1: Introduction

Purpose

This document provides information you need to configure and use system monitoring for the Ethernet Routing Switch 5600 Series.

Related resources

Documentation

See the *Documentation Reference for Avaya Ethernet Routing Switch 5000 Series*, NN47200–103 for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com.

Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and check the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: New in this release

The following sections detail what's new in *Configuring System Monitoring on Avaya Ethernet Routing Switch 5000 Series*, NN47200-505 for Release 6.6.

Features

See the following sections for information about feature changes.

Remote Switch Port Analyzer (RSPAN)

Remote Switch Port Analyzer (RSPAN), also known as Remote Port Mirroring, enhances port mirroring by enabling mirrored traffic to be sent to one or more switches or stacks on the network.

For more information, see in this guide:

- Remote Switch Port Analyzer (RSPAN) on page 25
- Configuring Remote Switch Port Analyzer (RSPAN) using ACLI on page 67
- Configuring Remote Switch Port Analyzer (RSPAN) using EDM on page 107

Show TCP Ports

You can view information about active IPv4 sockets similar to the output from the Unix netstat command.

For more information, see in this guide:

- Displaying TCP ports on page 53

SLA Monitor

The Service Level Agreement (SLA) Monitor is an embedded monitoring device designed to identify and isolate performance issues in a network.

For more information, see in this guide:

- SLA Monitor on page 33
- Configuring the SLA Monitor using ACLI on page 165
- Configuring the SLA Monitor using EDM on page 175

Other changes

See the following sections for information about changes that are updates to previously existing information.

CLI interface change from FastEthernet to Ethernet

The CLI interface command `interface FastEthernet` is changed to `interface Ethernet`. The FastEthernet interface command remains available, but hidden so as to provide backward compatibility.

Comments? infodev@avaya.com

Chapter 3: System monitoring fundamentals

System monitoring is an important aspect of switch operation. The Avaya Ethernet Routing Switch 5000 Series provides a wide range of system monitoring options that you can use to closely monitor the operation of a switch or stack.

This chapter describes two general system monitoring aspects that you must consider when you use the Avaya Ethernet Routing Switch 5000 Series: system logging and port mirroring. Subsequent chapters provide information about specific system monitoring tools and how to use them.

System logging

The Avaya Ethernet Routing Switch 5000 Series supports system logging (syslog), a software tool to log system events for debugging and analysis.

The syslog tool can log application events. The logged events are stored in volatile RAM, nonvolatile RAM, or in a remote host. You can select the storage location by using the Avaya Command Line Interface (ACLI) or Enterprise Device Manager (EDM).

Remote logging

The remote logging feature provides an enhanced level of logging by replicating system messages on a syslog server. System log messages from several switches can be collected at a central location to alleviate you from individually querying each switch to interrogate the log files.

You must configure the remote syslog server on the unit to log informational, serious, and critical messages to this remote server. The UDP packet is sent to port 514 of the configured remote syslog server.

You can configure the remote logging facility of all logged messages. If you do not specify the facility, the default facility is daemon.

After the IP address is in the system, syslog messages can be sent to the remote syslog server. If a syslog message is generated prior to capturing the IP address of the server is captured the system stores up to 30 messages that are sent after the IP address of the remote server is on the system.

To configure this feature, enable remote logging, specify the IP address of the remote syslog server, and specify the severity level of the messages to be sent to the remote server.

Note:

- If you specify the informational level, then informational, serious, and critical messages will be sent to the remote syslog server
- If you specify the serious level, then serious and critical messages will be sent to the remote syslog server
- If you specify the critical level, then only critical messages will be sent to the remote syslog server

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 logged, even if one of the servers becomes unavailable.

Alarms

Alarms are useful for identifying values of a variable that have gone out of range. Define an RMON alarm for a MIB variable that resolves to an integer value. String variables cannot be used. 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.

After alarms are activated, view the activity in a log or a trap log, or a script can be created to provide notification by beeping a console, sending e-mail messages, or calling a pager.

How RMON alarms work

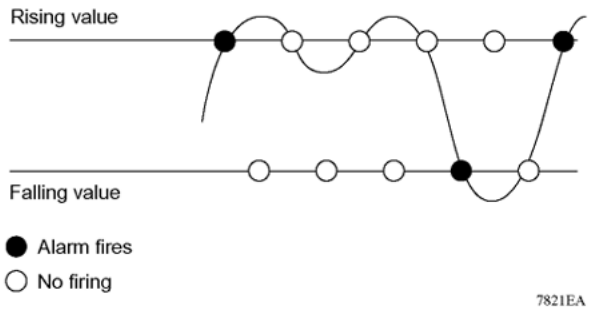
The alarm variable is polled and the result is compared against upper and lower limit values you select after you create the alarm. If either limit is reached or crossed during the polling period; then the alarm fires and generates an event that you can view in the event log or the trap log.

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*

Comments? infodev@avaya.com

interval that the data passes above the rising value, the alarm fires as a rising event. During the first interval that the data drops below the falling value, the alarm fires as a falling event.

The following figure describes how alarms fire.



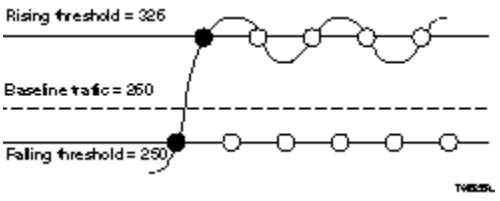
The alarm fires during the first interval that the sample goes out of range. No additional events are generated for that threshold until the opposite threshold is crossed. Therefore, it is important to carefully define the rising and falling threshold values for alarms to work as expected. Otherwise, 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 will cause the value for outbound octets to drop to zero), the falling alarm cannot fire because the baseline traffic is always greater than the value of the falling threshold. By definition, the failure of the falling alarm to fire prevents the rising alarm from firing a second time.

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



Creating alarms

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

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

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

Trap Web page

SNMP Trap web page provides a graphical method to enable or disable traps you want to send. In case multiple trap receivers are selected you can specify which traps are sent to which receiver. The selection of traps to be sent to a certain receiver can be based on criteria like security, network connectivity, or other information that might be important to that particular receiver.

You can access a separate Trap web page for every host, from which you can enable or disable any of the listed traps. The access to those pages is through the SNMP Trap Web page, which contains two options for every trap. The first option enables the trap. The second option disables the trap. Select an option to enable or disable a specific trap for a specific host.

Comments? infodev@avaya.com

Management Information Base Web page

With Web-based management, you can see 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:

- SNMP SET requests
- displaying SNMP tables
- translating MIB enumerations that are displaying the name (interpretation) of number values of objects defined as enumerations in the MIB

IGMP and the system event log

IGMP uses the components provided by the syslog tool. The syslog tool performs functions, such as storing messages in the NVRAM or remote host and displaying these log messages through the ACLI, console menu, or Telnet.

The IGMP log events can be in one of the following three categories based on their severity:

- Critical
- Serious
- Informational

IGMP logs the messages whenever any of the following types of events occur in the system:

- IGMP initialization
- Configuration changes from the user
- Stack Join events
- IGMP messages: Report, Leave and Query messages received by the switch

Events such as reception of IGMP messages occur frequently in the switch whenever a new host joins or leaves a group. Logging such messages consumes a large amount of log memory.

Therefore, such messages should not be logged in all the time. By default, such message logging is disabled. You must enable this feature through the ACLI to view the messages.

In Table 1: IGMP syslog messages on page 20:

- %d represents a decimal value for the preceding parameter. For example, 5 for VLAN 5
- %x represents a hexadecimal value for the preceding parameter. For example, 0xe0000a01 for Group 224.0.10.1

Table 1: IGMP syslog messages on page 20 describes the IGMP syslog messages and the severity.

Table 1: IGMP syslog messages

Severity	Log messages
Informational	IGMP initialization success
Critical	IGMP initialization failed: Error code %d
Informational	IGMP policy initialized
Informational	IGMP configuration loaded successfully
Informational	IGMP configuration failed. Loaded to factory default
Informational	IGMP configuration changed: Snooping enabled on VLAN %d
Informational	IGMP configuration changed: Snooping disabled on VLAN %d
Informational	IGMP configuration changed: Proxy enabled on VLAN %d
Informational	IGMP configuration changed: Proxy disabled on VLAN %d
Informational	IGMP configuration changed: Query time set to %d on VLAN %d
Informational	IGMP configuration changed: Robust value set to %d on VLAN %d
Informational	IGMP configuration changed: Version %d router port mask 0x%x set on VLAN %d
Informational	IGMP configuration changed: Unknown multicast filter enabled
Informational	IGMP configuration changed: Unknown multicast filter enabled
Informational	IGMP configuration changed: Trunk %d created for IGMP
Informational	IGMP configuration changed: Trunk %d removed for IGMP ports
Informational	IGMP configuration changed: Mirror ports set
Informational	IGMP configuration changed: Port %d added to VLAN %d
Informational	IGMP configuration changed: Port %d removed from VLAN %d
Informational	IGMP new Querier IP %x learned on port %d
Informational	IGMP exchange database sent by unit %d
Informational	IGMP exchange database received on unit %d from %d
Informational	IGMP exchange database done
Informational	IGMP stack join completed

Comments? infodev@avaya.com

Severity	Log messages
Serious	IGMP not able to join stack: Error code %d
Informational	IGMP exchange group database sent by unit %d
Informational	IGMP exchange group database received on unit %d from %d
Informational	IGMP received report on VLAN %d for Group 0x%x on port %d
Informational	IGMP received leave on VLAN %d for Group 0x%x on port %d
Informational	IGMP received query on VLAN %d for Group 0x%x on port %d
Informational	IGMP dynamic router port %d added
Informational	IGMP dynamic router port %d removed

Port mirroring

You can designate a switch port to monitor traffic on any other specified switch ports (port-based) or to monitor traffic to or from any two specified addresses that the switch learned (address-based).

A probe device, such as the Avaya StackProbe or equivalent, must connect to the designated monitor port to use this feature. Contact an Avaya sales agent for details about the StackProbe.

Port-based mirroring configuration

Figure 1: Port-based mirroring example on page 22 shows an example of a port-based mirroring configuration in which port 20 is designated as the monitor port for ports 21 and 22 of Switch S1. Although this example shows ports 21 and 22 monitored by the monitor port (port 20), any trunk member of T1 and T2 can also be monitored.

In this example, Figure 1: Port-based mirroring example on page 22 shows port X and port Y as members of Trunk T1 and Trunk T2. Port X and port Y are not required to always be members of Trunk T1 and Trunk T2.

You cannot monitor trunks and you cannot configure trunk members as monitor ports.

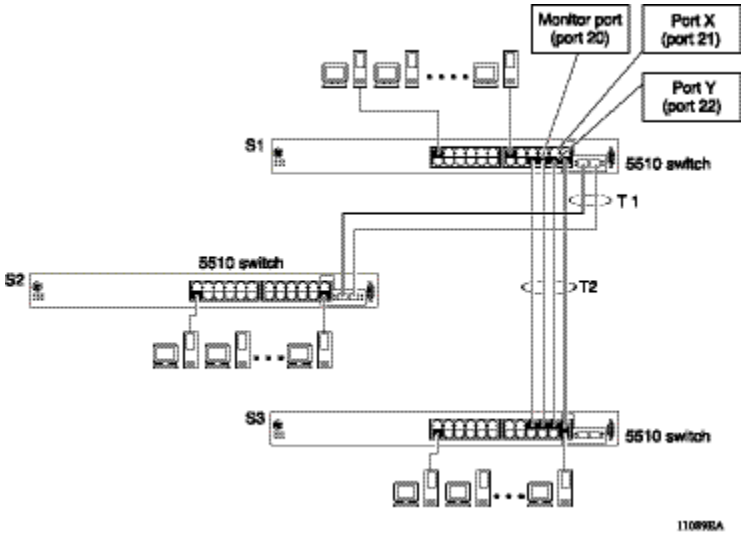


Figure 1: Port-based mirroring example

In the preceding configuration example, you can configure the designated monitor port (port 20) to monitor traffic in any of the following modes:

- Monitor all traffic received by port X.
- Monitor all traffic transmitted by port X.
- Monitor all traffic received and transmitted by port X.
- Monitor all traffic received by port X or transmitted by port Y.
- Monitor all traffic received by port X (destined to port Y) and then transmitted by port Y.
- Monitor all traffic received or transmitted by port X and transmitted or received by port Y (conversations between port X and port Y).
- Monitor all traffic received on many ports.
- Monitor all traffic transmitted on many ports.
- Monitor all traffic received or transmitted on many ports.

Address-based mirroring configuration

The following example shows an address-based mirroring configuration in which port 20, the designated monitor port for Switch S1, monitors traffic occurring between address A and address B.

Comments? infodev@avaya.com

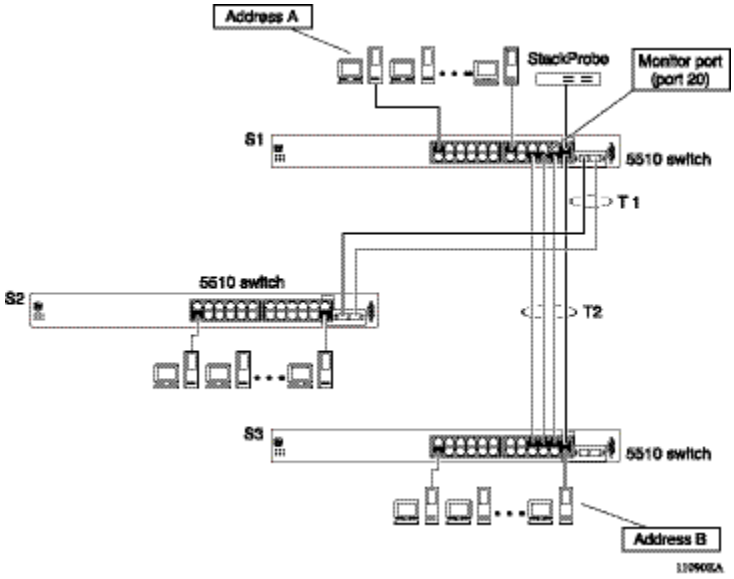


Figure 2: Address-based mirroring example

In this configuration, the designated monitor port (port 20) can be set to monitor traffic in any of the following modes:

- Monitor all traffic transmitted from address A to any address.
- Monitor all traffic received by address A from any address.
- Monitor all traffic received by or transmitted by address A.
- Monitor all traffic transmitted by address A to address B.
- Monitor all traffic between address A and address B (conversation between the two stations).

Bi-directional Monitor Port

With this feature, you can configure the monitor port (MTP) to participate in bi-directional traffic flows. A device with intrusion detection software (IDS) or intrusion protection software (IPS) or with both, and connected to the monitor port, can recognize a traffic threat and initiate a session to disable the port. Mono-directional traffic flow is the default. Avaya recommends that you enable this feature only if the devices to connect through MTP use telnet, SSH, or SNMP.

Many-to-Many Port Mirroring

Many-to-Many Port Mirroring is an extension of the Port Mirroring application, to allow multiple sessions of mirroring configuration to exist simultaneously, each with a Monitor Port and mirrored ports.

You can configure this the feature by using ACLI. The configuration process for each instance is similar to Port Mirroring configuration.

Port-based modes

The following port-based modes are supported:

- ManytoOneRx: Many-to-One port mirroring on ingress packets.
- ManytoOneTx: Many to one port mirroring on egress packets.
- ManytoOneRxTx Many to one port mirroring on ingress and egress traffic.
- Xrx: Mirror packets received on port X.
- Xtx: Mirror packets transmitted on port X.
- XrxOrXtx: Mirror packets received or transmitted on port X.
- XrxYtx: Mirror packets received on port X and transmitted on port Y.
- XrxYtxOrYrxXtx: Mirror packets received on port X and transmitted on port Y or packets received on port Y and transmitted on port X.
- XrxOrYtx: Mirror packets received on port X or transmitted on port Y

MAC address-based modes

- Asrc: Mirror packets with source MAC address A.
- Adst: Mirror packets with destination MAC address A
- AsrcOrAdst: Mirror packets with source or destination MAC address A.
- AsrcBdst: Mirror packets with source MAC address A and destination MAC address B.
- AsrcBdstOrBsrcAdst: Mirror packets with source MAC address A and destination MAC address B or packets with source MAC address B and destination MAC address A.

Many-to-many port mirroring functionality

Many-to-Many Port Mirroring builds on the existing Port Mirroring application. Multiple instances are each configurable by using the existing interface. Each instance is attached to one Monitor Port (MTP). In some cases a monitor port can be used in more than one instance. Up to four instances are available.

The ports which are configured as MTP are not allowed to be part of a MLT group.

Comments? infodev@avaya.com

Many-to-many port mirroring restrictions

Many-to-Many Port Mirroring is available on Ethernet Routing Switch 5600 Series.

An MTP cannot be a mirrored port for another MTP. Frames mirrored to one MTP are not taken into account in MAC address-based mirroring on another MTP.

A port cannot be configured as MTP in an instance if it is already a mirrored port in another instance.

If a port is egress-mirrored in one instance, it cannot be egress-mirrored in another instance (to another MTP). The same applies to ingress-mirrored ports. A port can be ingress-mirrored in one instance and egress-mirrored in another.

The ports that are configured as MTP cannot participate in a normal frame switching operation.

Remote Switch Port Analyzer (RSPAN)

Remote Switch Port Analyzer (RSPAN), also known as Remote Port Mirroring, enhances port mirroring by enabling mirrored traffic to be sent to one or more switches or stacks on the network. All participating switches must support the RSPAN feature.

For each RSPAN session, the mirrored traffic is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches.

RSPAN consists of at least one RSPAN source session, an RSPAN VLAN and at least one RSPAN destination session. The RSPAN traffic from the source ports is copied into the RSPAN VLAN and forwarded to a destination session monitoring the RSPAN VLAN. The final destination must always be a physical port on the destination switch. You can also include intermediate switches separating the RSPAN source and destination sessions. You separately configure RSPAN on the source switch, the intermediate switch(es) and destination switch. You must create an RSPAN VLAN on each device involved in an RSPAN session.

RSPAN VLAN is a port based VLAN, carrying traffic between RSPAN source and destination sessions. You can have multiple RSPAN VLANs in a network at the same time, with each RSPAN VLAN defining a network-wide RSPAN session.

You can configure up to 4 RSPAN VLANs on a switch.

For a minimal RSPAN configuration, you need:

- one RSPAN port on a source RSPAN session
- two ports on a destination RSPAN session (one port as a network port and one as an RSPAN destination port).

Note:

On an intermediate switch, Avaya recommends that you configure up to 12 ports.

Note:

Due to hardware limitations, RSPAN is not compatible with VSP 9000 or ERS 8800.

There is no hardware support for the RSPAN VLAN on 55xx or 45xx units.

RSPAN source sessions

To configure an RSPAN source session on a source switch, you associate a port mirroring instance with an RSPAN VLAN. The output of this session is a stream of packets sent to the RSPAN VLAN. An RSPAN source session is very similar to a local port mirroring session, except that the packet stream is directed to the RSPAN VLAN. In an RSPAN instance, the mirrored packets are supplementary tagged with the RSPAN VLAN ID and directed to the destination switch. When exiting the source switch, the RSPAN traffic has both vlan labels (double tagging).

You can have more than one source session active in the same RSPAN VLAN, each source session on a separate switch. Multiple RSPAN source sessions anywhere in the network can contribute packets to the RSPAN session.

RSPAN destination sessions

An RSPAN destination session presents a copy of all RSPAN VLAN packets (except Layer 2 control packets) to the user for analysis.

To configure an RSPAN destination session on a destination switch, you associate the destination port with the RSPAN VLAN. The destination session collects all RSPAN VLAN traffic and sends it out the designated RSPAN destination port. An RSPAN destination session takes all packets received on the RSPAN VLAN, strips off the VLAN tagging, and presents them on the destination port.

You can have more than one destination session active in the same Cisco compatible RSPAN VLAN. You can monitor the same RSPAN VLAN with multiple RSPAN destination sessions throughout the network. In this situation, you can consider the RSPAN VLAN ID as a network wide ID for a particular monitoring session.

When configuring an RSPAN destination session, if the destination port is not part of the RSPAN VLAN, the port is automatically moved in the RSPAN VLAN and set to untagged. If a previous VLAN configuration prevents port moving, an error message is displayed.

When an RSPAN destination interface is erased, the RSPAN port is removed from the RSPAN vlan and set to untagged state.

You can configure up to 4 RSPAN destination instances on a destination switch. Each RSPAN instance holds a single destination port, meaning that you can configure up to 4 destination ports on a switch.

Note:

The RSPAN destination session does not occupy one of the four standard port-mirroring sessions. You can still configure up to 4 port-mirroring sessions on the destination switch.

RSPAN restrictions and interactions with other features

RSPAN interacts with the following features:

VLAN interactions

- No MAC address learning occurs on the RSPAN VLAN, because all RSPAN VLAN traffic is always flooded.
- Mapping of an RSPAN VLAN over an SPB ISID and transport over an SPB cloud is not supported.
- You cannot:
  - remove an RSPAN destination port from the RSPAN VLAN while this port is involved in the RSPAN instance
  - remove an RSPAN VLAN if it is used in an RSPAN instance. You must disable the RSPAN instance first
  - change the membership of an RSPAN destination port without disabling first the instance
  - set a SPBM B-VLAN or a spbm-switchedUni VLAN as an RSPAN VLAN
  - set an RSPAN VLAN as a management VLAN
  - use the same vlan or the same interface in another RSPAN destination instance
  - use the same interface for the same vlan in another RSPAN source instance

Port mirroing

- Port Mirroring general limitations regarding VLAN tagging also apply to RSPAN.
- You can specify any ports within the stack as ports for RSPAN port-mirroring sessions, with the following exceptions:

  You cannot:
  - configure a port which has 802.1X enabled as an RSPAN destination port.
  - configure a port which is a member of MLT/DMLT/LAG as an RSPAN destination port.
  - configure a port which is a member of MLT/DMLT/LAG as a port mirroring/RSPAN source.
  - configure a port as an RSPAN destination or Mirror To Port (MTP) if this port is an RSPAN source / mirrored port for another instance.
  - configure the allow-traffic option for port-mirroring along with RSPAN
- For MAC base modes: Asrc, Adst, AsrcBdst, AsrcBdstOrBsrcAdst, AsrcOrAdst and port based modes: XrxYtx, XrxYtxOrYrxXtx port-mirroring, you must install filters to enable port mirroring/ RSPAN source. If platform resource limits are reached the application may not function in these modes.
- For port based modes XrxYtx, XrxYtxOrYrxXtx RSPAN will only work for unicast traffic. Broadcast/Multicast/UUC traffic does not use hardware filters, it uses a group of workarounds that must be removed in order for RSPAN to work.

- Port-mirroring shows incorrect source/dest mac for routed Layer 3 traffic, as the Mirroring is the last operation performed by the ASIC (ie after routing).
- In a stack scenario with a port configured on a unit that is powered off, the port will still be displayed for the "show port-mirroring [rspan]" command(s). However, those ports are functional only if the units they belong to are powered on, otherwise they cannot be used for mirroring in any scenario. After power off, if the setup becomes a single unit, the ports displayed may be mistaken with a normal configuration since the unit will not be displayed anyhow for a single box. In order to avoid this confusion, if there is no intention of powering off the non-base units to go back to the stack scenario, Avaya recommends that you erase the port-mirroring preexisting settings.
- The RSPAN destination port is set as an untagged member of the RSPAN VLAN, to ensure that the RSPAN tag is stripped off.

STP interactions

- The RSPAN destination port does not participate in STP.
- The RSPAN destination port follows the same rules as a local MTP in regard to STP and topology packets.
- Control packets are mirrored by an RSPAN instance. The mirrored BPDUs may get mixed up with the actual BPDUs, resulting in STP loops and topology issues. Control packets are treated separately and may be discarded before reaching destination port.

Stack loopback tests

You can quickly test your stack ports and stack cable by using the stack loopback test. The stack loopback test is useful after you need to determine whether the source of the problem is a defective stack cable or a damaged stack port. The test can help prevent unnecessarily sending switches for service.

Two types of loopback tests exist. The internal loopback test verifies that the stack ports are functional.

The external loopback test checks the stack cable to determine if it is the source of the problem. Perform the external loopback test by connecting the stack uplink port with the stack downlink port, sending a packet from the uplink port, and verifying that the packet is received on the downlink port.

Always run the internal test first, because the cable tests are not conclusive until you ensure the stack ports work correctly.

Warning:

Perform the loopback tests in the standalone mode to avoid any impact on the stack functioning.

Comments? infodev@avaya.com

Stack monitor

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

The stack monitor sends a trap for the following events.

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

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

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

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

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 device displays diagnostic and operation information though the Light Emitting Diodes (LED) on the unit. Familiarize yourself with the interpretation of the LEDs on the Avaya Ethernet Routing Switch 5000 Series device. For information about the LED display see *Installing the Avaya Ethernet Routing Switch 5000 Series*, NN47200-300.

Power over Ethernet allocations

Devices such as IP phones, Web cameras, wireless access points that utilize Power over Ethernet (PoE). The switch displays the PoE allocations for each port. The PoE standard (802.3af) imposes the Power Devices (PD) that require power to run at 48 V and not draw more than 16 W.

The switch has multiple ports that are PoE capable. You must make consideration for the total power and maximum power provided required for each port and unit. Another important aspect is that of device priority. You must decide which device receives power when there is not enough for all.

Use the syslog to check the parameters. The following traps are logged:

- pethPsePortOnOffNotification: indicates if the switch port delivers power to the connected device. This notification is sent on every status change except in the search mode.
- pethMainPowerUsageOnNotification: indicates that the switch threshold usage indication is on and the usage power is higher than the threshold.
- pethMainPowerUsageOffNotification : indicates that the switch threshold usage indication is off and the usage power is lower than the threshold.

Displaying PoE allocations using ACLI

Use this procedure to display the PoE status for the switch.

Procedure Steps

1. Use the following command to display the overall status of PoE.

   ```
   show poe-main-status
   ```

2. Use the following command to display the port-level PoE status.

   ```
   show poe-port-status
   ```

3. Use the following command to display power allocations on the switch.

Comments? infodev@avaya.com

```
show poe-power-measurement
```

Displaying PoE allocations using EDM

Use the following procedure to display the PoE status for the switch.

1. From the navigation tree, double-click **Power Management**.
2. In Power Management tree, double-click **PoE**.
3. In the work area, click **Globals - PoE Units** tab to view overall PoE status on the switch.
4. Click **PoE Ports** tab to view port-level PoE information.

IP Flow Information Export

IP Flow Information Export (IPFIX) is a protocol used to export flow information from traffic observed on a switch. Because IPFIX is still in development with the IETF, the current implementation is based on Netflow Version 9.

IP traffic is sampled and classified into various flows based the following parameters:

- protocol type
- destination IP address
- source IP address.
- ingress port
- TOS

You can not use IPFIX on secondary interfaces.

If the protocol type is TCP or UDP, a flow is defined by two additional parameters:

- source port
- destination port

Release 5.0 and later supports IPFIX through the creation and display of sampled information as well as the ability to export this sampled information. You can access IPFIX accessed through Enterprise Device Manager (EDM).

The IPFIX feature shares resources with QoS. If the IPFIX feature is enabled, a QoS policy precedence is used. For further information about QoS policies, see the *Configuring Quality of Service on Avaya Ethernet Routing Switch 5000 Series*, NN47200-504.

Remote Network Monitoring

The Remote Network Monitoring (RMON) MIB is an interface between the RMON agent on the Avaya Ethernet Routing Switch 5000 Series and an RMON management application, such as the Device Manager.

RMON defines objects that are suitable for managing any type of network, but some groups are targeted specifically for Ethernet networks.

The RMON agent continuously collects statistics and monitors switch performance.

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

Debug trace commands

The trace feature provides useful information about the error events detected by the device. You can use this information to help you resolve an issue.

A trace command is available that is supported in OSPF, RIP, SMLT, IPMC, IGMP, PIM and 802.1X/EAP. Release 6.2 and beyond supports four levels of the trace command for each module or application:

- Very Terse
- Terse
- Verbose
- Very Verbose

Each succeeding level provides more detailed information on the specific module. You can enable or disable trace globally or independently for each module, and you can specify the trace level for each module. The system delivers the information from this command to the console screen.

Use trace only for active troubleshooting because it is resource intensive.

The ACLI supports this feature.

Comments? infodev@avaya.com

Stack Health Check

The Stack Health Check feature provides information on the stacking state of each switch rear port. It is used to run a high-level test to monitor the rear port status for each unit, confirm the number of switching units in stack, detect if the stack runs with a temporary base unit, and to monitor stack continuity.

This feature is available through the ACLI.

Displaying environmental information

This feature provides information on the status of the environment of each unit in a stack. It is used to perform the following tasks:

- Monitor the hardware status for each unit.
- Detect the presence of primary or redundant power.
- Monitor the CPUs temperature.
- Identify damaged or missing hardware.

SLA Monitor

The Ethernet Routing Switch 5600 Series supports the Service Level Agreement (SLA) Monitor agent as part of the Avaya SLAMon solution.

SLAMon uses a server and agent relationship to perform end-to-end network Quality of Service (QoS) validation. You can use the test results to target under-performing areas of the network for deeper analysis.

Server and agent

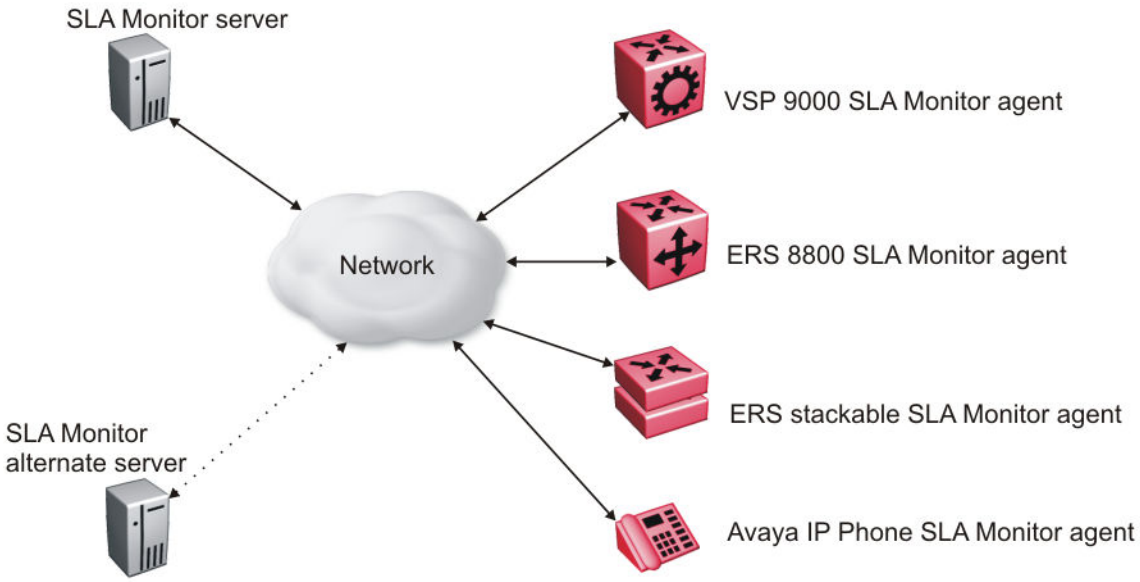
SLA Monitor agent performs QoS tests after it receives a request from the SLA Monitor server. The tests can be performed even if the server is not available.

The SLA Monitor server initiates the SLA Monitor functions on two or more agents. The agents run specific QoS tests at the request of the server. Agents exchange packets between one another to conduct the QoS tests. The test schedule and the exact nature and intensity of each test depends on the parameters that are configured on the server. The server stores the data

it collects from the agents about the network. SLA Monitor can monitor a number of key items, including the following:

- network paths
- Differentiated Services Code Point (DSCP) markings
- loss
- jitter
- delay

The following figure illustrates an SLA Monitor implementation



An SLA Monitor agent remains dormant until it receives a User Datagram Protocol (UDP) discovery packet from the server. The agent accepts the discovery packet to register with an SLA Monitor server. If the registration process fails, the agent remains dormant until it receives another discovery packet.

An agent can attempt to register with a server once every 60 seconds. After a successful registration, the agent will reregister with the server every 6 hours to exchange a new encryption key, if encryption is supported.

An agent only accepts commands from the server to which it is registered. An agent can use alternate servers to provide backup for timeout and communication issues with the primary server.

Secure agent-server communication

The secure SLA Monitor agent-server communication feature supports certificate-based authentication and encrypted agent-server communication. The communication mode is based on the ERS image. Secure images use authentication/encryption and non-secure images use clear text communication. Mocana security libraries are used for authentication and encryption. During registration, an X.509 certificate is retrieved from the server and then validated against the stored Avaya CA certificate. If the received certificate is trusted, a secure channel is

Comments? infodev@avaya.com

established. A symmetric encryption key is exchanged and used for all subsequent agent server communication.

Note:

The certificate-based authentication and encrypted agent-server communication is automatically enabled on secure ERS images. This feature cannot be configured by the user.

QoS tests

SLA Monitor uses two types of tests to determine QoS benchmarks:

- Real Time Protocol (RTP)

  This test measures network performance, for example, jitter, delay, and loss, by injecting a short stream of UDP packets from source to destination (an SLA Monitor agent).
- New Trace Route (NTR)

  This test is similar to traceroute but also includes DSCP values at each hop in the path from the source to the destination. The destination does not need to be an SLA Monitor agent.

SLA Monitor uses Real Time Protocol (RTP) and New Trace Route (NTR) tests to determine the Quality of Service (QoS) benchmarks. You can run the NTR and RTP tests through the platform CLI and EDM in the absence of an SLA Monitor server.

Tests are run serially and only one type of test can be run at a time. You can disable the SLA Monitor agent if the functionality is not required.

Note:

Command execution fails if you disable the SLA Monitor agent.

SLM CLI support

You can utilize components of the SLA Monitor agent without the use of a server through the SLM CLI. You can use the SLM CLI to initiate NTR and RTP tests, as well as to display agent status information.

Access to SLM CLI is available if the agent is enabled. Established sessions automatically time out after a specific interval (default interval is 60 seconds). You can enable/disable SLM CLI through the platform CLI as well as through EDM. You can also configure the session timeout value or disable it completely.

The SLM CLI support is primarily present for agent debugging.

Platform CLI SLAMon test access

In the absence of SLA Monitor server support, the SLAMon RTP and NTR tests are available from the platform CLI. The commands are simplified to highlight the essential functionality and test output is condensed. The platform CLI SLAMon NTR and RTP tests can be initiated even if the agent is not currently registered with a server.

You can execute only a single NTR or RTP test at any one time due to agent architecture restrictions. For this reason, synchronization across the platform CLI sessions, the SLM CLI and the server-initiated SLAMon tests is required. If a test request cannot be satisfied at a

given time, the switch reports a ‘busy’ message. Server test access can be temporarily blocked to get around a continually busy agent by disabling server test access through the platform CLI. Agents that are not registered may need to enable server bypass support to take part in certain tests.

Limitations

SLA Monitor agent communications are IPv4–based. Agent communications do not currently support IPv6.

For information on configuring the SLA Monitor agent, see

- Configuring the SLA Monitor using ACLI on page 165
- Configuring the SLA Monitor using EDM on page 175

Chapter 4: System diagnostics and statistics using ACLI

This chapter describes the procedures you can use to perform system diagnostics and gather statistics using ACLI.

Trace diagnosis of problems

The following sections describe how to use trace to diagnose problems.

Trace diagnosis of problems navigation

- Using trace to diagnose problems on page 37
- Viewing the trace level on page 39
- Viewing the trace module ID list on page 39

Using trace to diagnose problems

Use trace to observe the status of a software module at a given time.

Caution:
Risk of traffic loss

Using the trace tool inappropriately can cause primary CPU lockup conditions, loss of access to the switch, loss of protocols, and service degradation.

Procedure steps

1. Enter Global Configuration mode.
2. Set the trace level by using the following command:

```
trace level <1-7> <0-4>
```

3. Set the trace screen on by using the following command:

   ```
   trace screen enable
   ```

4. Set the trace screen off by using the following command:

   ```
   trace screen disable
   ```

5. Disable the trace by using the following command:

   ```
   trace shutdown
   ```

Variable definitions

Use the data in the following table to help you use the trace feature.

Variable	Value
`level <1-7> <0-4>`	Sets the trace level: • *<1-7>* sets the trace module ID list: - 1 is OSPF - 2 is IGMP - 3 is PIM - 4 is RIP - 5 is SMLT - 6 is IPMC - 7 is NTP • *<0-4>* sets the trace level: - 0 indicates that the trace is disabled. - 1 is very terse. - 2 is terse. - 3 is verbose. - 4 is very verbose.
`screen <enable | disable>`	Enables or disables the trace screen. You can use this command to control the trace output to the console. The default is disable.
`shutdown`	Disables the trace. Shutdown sets all the modules level to 0, and produces a "NO_DISPLAY" message.

Comments? infodev@avaya.com

Viewing the trace level

Use this procedure to view the trace level information for the modules.

Procedure steps

1. Enter the Privileged EXEC mode.
2. DIsplay the trace level by using the following command:

   ```
   show trace level
   ```

Job aid

The following table describes the fields for the **`show trace level`** command.

Variable	Value
TraceModId	Indicates the Trace mode ID.
Name	Indicates the name of the mode.
Level	Indicates the trace level. • 1 is very terse. • 2 is terse. • 3 is verbose. • 4 is very verbose.

Viewing the trace module ID list

Use this procedure to view the supported module list for the trace feature.

Procedure steps

1. Enter the Privileged EXEC mode.
2. Display the trace module ID list by using the following command:

   ```
   show trace modid-list
   ```

Job aid

The following table describes the fields for the **show trace modid-list** command.

Variable	Value
TraceModID	Indicates the trace module ID.
ModId	Indicates the ID of the module.
Name	Indicates the name of the module.

Port statistics

Use the ACLI commands in this section to derive port statistics from the switch.

Viewing port-statistics

Use this procedure to view the statistics for the port on both received and transmitted traffic.

Procedure steps

1. Enter Global Configuration mode.
2. Enter the following command:

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

Variable definitions

The following table describes the command parameters.

Variable	Definition
port <portlist>	The ports to display statistics for. When no port list is specified, all ports are shown.

Configuring Stack Monitor

The following ACLI commands are used to configure the Stack Monitor.

Comments? infodev@avaya.com

Viewing the stack-monitor

Use this procedure to display the status of the Stack Monitor.

Procedure Steps

1. Enter Privileged Executive mode.
2. Enter the following command:

```
show stack monitor
```

Variable definitions

The following is an example of the **`show stack monitor`** command output.

```
5698TFD#show stack-monitor
Status: disabled
Stack size: 2
Trap interval: 60
5698TFD#
```

Configuring the stack-monitor

Use this procedure to configure the Stack Monitor.

Important:

If you do not specify a parameter for this command, all Stack Monitor parameters are set to their default values.

Procedure Steps

1. Enter Global Configuration mode.
2. Enter the following command:

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

Table 2: Variable Definitions

Variable	Definition
enable	Enables stack monitoring.
stack-size <2-8>	Sets the size of the stack to monitor. Valid range is from 2 to 8. By default the stack size is 2.

Variable	Definition
trap-interval <30-300>	Sets the interval between traps, in seconds. Valid range is from 30 to 300 seconds. By default the trap-interval is 60 seconds.

Setting default stack-monitor values

Use this procedure to set the Stack Monitor parameters to their default values.

Configuring default stack monitor using ACLI

1. Enter Global Configuration mode.
2. Enter the following command:

```
default stack-monitor
```

Disabling the stack monitor

Use this procedure to disable the stack monitor.

Procedure Steps

1. Enter Global Configuration mode.
2. Enter the following command:

```
no stack monitor
```

Viewing Stack Port Counters

Use this procedure to configure the stack port counters.

Important:

The stack counters measure the size of packets received on HiGig ports. The size of these packets is greater than the size of the packets received on front panel ports since ASIC HiGig+ header is added to each of them. The size of this header is 12 bytes, therefore another range of stack counters is incremented when sending packets having length close to the stack counters upper intervals limit.

Comments? infodev@avaya.com

Important:

The number of received/transmitted packets can be greater than the number of packets transmitted on front panel ports since there are different stack management packets transmitted/received.

Procedure Steps

Use the following command to show stacking statistics:

```
show stack port-statistics [unit <1-8>]
```

Variable Definitions

The following table describes the command parameters.

Variable	Definition
unit <1-8>	Specifies the unit in the stack.

Job aid

The following tables describes the output from the show stack port-statistics command.

Received	UP	DOWN
Packets	1052	391283
Multicasts	1052	1582
Broadcasts	0	94
Total Octets	1869077	29862153
Packets 64 bytes	0	389600
65-127 bytes	204	763
128-225 bytes	21	27
256-511 bytes	409	492
512-1023 bytes	2	18
1024-1518 bytes	18	19
Jumbo	398	364
Control Packets	0	0
FCS Errors	0	0
Undersized Packets	0	0

Received	UP	DOWN
Oversized Packets	0	0
Filtered Packets	0	0

Transmitted	UP	DOWN
Packets	1257	1635
Multicasts	1246	1624
Broadcasts	11	11
Total Octets	407473	1765434
FCS Errors	0	0
Undersized Packets	0	0
Pause Frames	0	0
Dropped On No Resources	0	0

Clearing stack port counters

Use the following procedure to clear the stack port counters

Procedure Steps

Use the following command to clear stacking statistics:

```
clear stack port-statistics [unit <1-8>]
```

Variable	Definition
unit <1-8>	Specifies the unit in the stack.

Using the stack loopback test

Use this procedure to complete a stack loopback test.

Configuring stack loopback test using ACLI

1. Enter Privileged Executive mode.
2. Enter the following command:

Comments? infodev@avaya.com

```
stack loopback-test internal
```

3. Enter the following command.

```
stack loopback-test external
```

Job aid

If a problem exists with a units stack port or a stack cable, an internal loopback test using the **stack loopback-test internal** command is performed. If the test displays an error then the stack port is damaged.

If the internal test passes, the external test can be run using the **stack loopback-test external** command. If the test displays an error then the stack cable is damaged.

The output of the **stack loopback-test internal** command is as follows:

```
5698TFD#stack loopback-test internal
Testing uplink port … ok
Testing downlink port … ok
Internal loopback test PASSED.
5698TFD#
5698TFD#stack loopback-test external
 External loopback test PASSED.
 5698TFD#
```

If one of the stack ports is defective (for example, such as the uplink), the output of the internal loopback test is as follows:

```
5698TFD#stack loopback-test internal
Testing uplink port … Failed
Testing downlink port … ok
Internal loopback test FAILED.
5698TFD#
```

If both the stack ports are functional, but the stack cable is defective, the external loopback test detects this, and the output is as follows:

```
5698TFD#stack loopback-test external
External loopback test FAILED. Your stack cable might be damaged.
5698TFD#
```

If you run the command on any unit of a stack, you see the following error message:

```
5698TFD#stack loopback-test internal
Stack loopback test affects the functioning of the stack.
You should run this in stand-alone mode
5698TFD#stack loopback-test external
Stack loopback test affects the functioning of the stack.   You
should run this in stand-alone mode
```

Displaying port operational status

Use this procedure to display the port operational status.

Important:

If you use a terminal with a width of greater than 80 characters, the output is displayed in a tabular format.

Procedure Steps

1. Enter Privileged Executive mode.
2. Enter the following command. If you issue the command with no parameters the port status is shown for all ports.

   ```
   show interfaces [port list] verbose
   ```

Validating port operational status

EAP: Configure EAP status to be unauthorized for some ports from ACLI. When you type **`show interfaces`**, EAP Status is Down for those ports.

VLACP: Configure VLACP on port 1 from a 5000 series unit and on port 2 on another 5000 series unit. Have a link between these 2 ports. When **`show interfaces`** command is typed, VLACP status is up for port on the unit where the command is typed. Pull out the link from the other switch, VLACP status goes Down.

STP: After switch boots, type **`show interfaces`** command. STP Status is Listening (wait a few seconds and try again). STP Status becomes Learning.

After a while (15 seconds is the forward delay default value, only if you did not configure another time interval for STP forward delay), if you type **`show interfaces`** again, STP Status should be forwarding.

Showing port information

Perform this procedure to display port configuration information.

Comments? infodev@avaya.com

Procedure Steps

1. Enter Privileged Executive mode.
2. Enter the following command:

   ```
   show interfaces <portlist> config
   ```

Job aid

The following is an example of the **show interfaces <portlist> config** command.

```
5650TD-PWR#show interfaces 1/1-2 config
Unit/Port:  1/1
Trunk:
Admin:  Enable
Oper Status:  Down
EAP Oper Status:  Up
VLACP Oper Status:  Down
STP Oper Status:  Forwarding
Link:  Down
LinkTrap:  Enabled
Link Autonegotiation:  Enabled
Energy Saver: Disabled
Energy Saver Oper Status: No Power Saving
BPDU-guard (BPDU Filtering): Disabled
BPDU-guard (BPDU Filtering) Oper Status: N/A
SLPP-guard: Enabled
SLPP-guard Oper Status: N/A

Unit/Port:  1/2
Trunk:
Admin Status:  Enable
Oper Status:  Down
EAP Oper Status:  Up
VLACP Oper Status :  Down
STP Oper Status :  Forwarding
Link:  Down
LinkTrap:  Enabled
Link Autonegotiation:  Enabled
Energy Saver: Disabled
Energy Saver Oper Status: No Power Saving
BPDU-guard (BPDU Filtering): Disabled
BPDU-guard (BPDU Filtering) Oper Status: N/A
SLPP-guard: Enabled
SLPP-guard Oper Status: N/A
```

Table 3: VLAN interfaces configuration

	Filter Untagged	Filter Unregistered				
Unit/Port	Frames	Frames	PVID	PRI	Tagging	Name
1/1	No	Yes	1	0	UntagAll	Unit 1, Port 1
1/2	No	Yes	1	0	UntagAll	Unit 1, Port 2

Table 4: VLAN ID port member configuration

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/1	1	VLAN #1				
1/2	1	VLAN#1				

Table 5: Spanning-tree port configurations

Unit	Port	Trunk	Participation	Priority	Path Cost	State
1	1	Normal	Learning	128	1	Forwarding
1	2	Normal	Learning	128	1	Forwarding

Showing stack health information

Perform this procedure to display stack health information.

Procedure steps

1. Enter Privileged Executive mode.
2. Enter the following command:

```
show stack health
```

Job aid

The following is an example of the **`show stack health`** command output when the stack is formed but did not end the initialization process.

```
#show stack health
Stack in progress
```


Comments? infodev@avaya.com

The following is an example of the **show stack health** command output when the stack is formed and initialized, and all the rear ports are up.

```
#show stack health
------------------------------------------------------------
-
Unit#       Switch Model         Cascade Up      Cascade Down
------------------------------------------------------------
--
1 (Base)     5698TFD-PWR              OK             OK
2            5650TD                   OK             OK
3            5698TFD                  OK             OK
------------------------------------------------------------
--
Switch Units Found = 3
Stack Health Check = OK - RESILIENT
Stack Diagnosis = Stack in full resilient mode
```

The following is an example of the **show stack health** command output when the stack is formed and initialized, and there are damaged or missing rear links.

```
#show stack health
------------------------------------------------------------
-
Unit#       Switch Model         Cascade Up      Cascade Down
------------------------------------------------------------
--
1 (Base)     5698TFD-PWR              OK             OK
2            5650TD                   OK             LINK DOWN OR MISSING
3            5698TFD                  OK             LINK DOWN OR MISSING
------------------------------------------------------------
--
Switch Units Found = 3
Stack Health Check = WARNING - NON-RESILIENT
Stack Diagnosis = Stack in non-resilient mode
Recommend to add/replace the identified cable(s).
```

The following is an example of the **show stack health** command output when the stack is formed and some of the rear ports are not functioning properly.

```
#show stack health
------------------------------------------------------------
-
Unit#       Switch Model         Cascade Up      Cascade Down
------------------------------------------------------------
--
1 (Base)     5698TFD-PWR              OK             OK
2            5650TD                   OK             UP WITH ERRORS
3            5698TFD           UP WITH ERRORS        OK
------------------------------------------------------------
--
Switch Units Found = 3
Stack Health Check = WARNING - NON-RESILIENT
Stack Diagnosis = Stack in non-resilient mode
Recommend to add/replace the identified cable(s).
```

A cable is not considered problematic (`UP WITH ERRORS`) when the switch connected to the other side is up but not in stack, or when the switch connected to the other side is up and in stack. A cable is considered problematic after several changes of status (between `OK` and `LINK DOWN`) occur in a short amount of time.

The following is an example of **show stack health** command output when the stack is running with a temporary base.

```
#show stack health
-------------------------------------------------------------
-
Unit#       Switch Model         Cascade Up      Cascade Down
-------------------------------------------------------------
--
1            5698TFD-PWR              OK             OK
2 (Temporary Base) 5650TD             OK             OK
3            5698TFD                  OK             OK
-------------------------------------------------------------
--
Switch Units Found = 3
Stack Health Check = OK - RESILIENT
Stack Diagnosis = Stack in full resilient mode.
```

The following is an example of the **show stack health** command output when the stack is formed and initialized and there are damaged or missing rear links and a temporary base unit.

```
#show stack health
-------------------------------------------------------------
-
Unit#       Switch Model         Cascade Up      Cascade Down
-------------------------------------------------------------
--
2(Temporary Base) 5698TFD-PWR LINK DOWN OR MISSING  OK
3            5650TD                  OK             OK
4            5698TFD                 OK LINK DOWN OR MISSING
-------------------------------------------------------------
--
Switch Units Found = 3
Stack Health Check = WARNING - NON-RESILIENT WITH TEMPORARY BASE
Stack Diagnosis = Stack in non-resilient mode, with temporary base unit.
Recommend replacing failed base unit or to add/replace the identified cables.
```

Job aid

Perform this procedure to ensure that the stack has the correct number of switching units and that it is running in resilient mode. If the stack is not running in resilient mode, use this procedure to identify damaged or missing cables and to repair faulty stacks.

Procedure steps

1. Display the stack health status from the ACLI.
2. If the number of units is the same as expected and the stack is resilient, this procedure is complete.
3. If the number of units is the same as expected, but the stack is not resilient, add or replace the identified cables and repeat the entire procedure.

Comments? infodev@avaya.com

4. If the number of units is not the same as expected, ensure all switching units are present and running and that they are properly connected.
5. If all the units are operational, but the number of units is not properly shown, remove or replace the units that do not appear.

Displaying the agent and image software load status using ACLI

Use the following procedure to display information about the diagnostic and agent code images on the switch. It displays both the installed and the operational agent.

Procedure

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

   ```
   show boot [image | diag]
   ```

Example

The following displays the output from the **`show boot [image | diag]`** command.

```
5650TD-PWR>enable
5650TD-PWR# show boot
Unit  Agent Image Secondary Image Active Image Diag Image Active Diag
----- ----------- --------------- ------------ ---------- -----------
1     6.6.0.47   6.3.0.020       6.3.0.047    6.0.0.4    6.0.0.4
* - Unit requires reboot for new Active Image to be made operational.
# - Unit requires reboot for new Diag to be made operational.
5650TD-PWR#show boot diag
Unit  Diag Image Active Diag
----- ---------- -----------
1     6.0.0.4     6.0.0.4
# - Unit requires reboot for new Diag to be made operational.
5650TD-PWR#show boot image
Unit  Agent Image Secondary Image Active Image
----- ----------- --------------- ------------
1     6.3.0.047   6.3.0.020       6.3.0.047
* - Unit requires reboot for new Active Image to be made operational.
5650TD-PWR#
```

Variable definitions

The following table describes the parameters associated with the **show boot** command.

Variable	Value
diag	Displays only information for the diagnostic load.
image	Displays only information for the image load.

Viewing environmental information

Perform this procedure to view the status of the unit or stack environment.

Procedure steps

1. Enter Privileged Executive mode
2. Enter the following command:

   show environmental

Job aid

The following is an example of the `show environmental` command output.

```
show environmental
Unit# PSU1      PSU2      FAN1 FAN2 FAN3 FAN4 FAN5 FAN6 Temperature
----- --------- --------- ---- ---- ---- ---- ---- ---- -----------
1     Primary   N/A       OK   OK   N/A  N/A  N/A  N/A  HIGH 43.5C


Unit# Model        Switch Capacity Saving PoE Saving
----- ------------ ---------------------- ------------------
1     5632FD       0.0 watts              N/A
-------------------------------------------------------------
TOTAL              0.0 watts              0.0 watts
=============================================
```

Job aid

Perform this procedure to ensure that the unit or stack works in proper conditions.

Comments? infodev@avaya.com

Procedure steps

1. Display the unit or stack environmental information from the ACLI.
2. If the information that appears indicates that each unit hardware environment is in good condition you have completed this procedure.
3. If the temperature is High or the fans have a Fail status, check the hardware.
4. Execute hardware maintenance.
5. Repeat steps 1 to 5 if necessary.

Displaying TCP ports

Use this procedure to display information about active IPv4 sockets similar to the output from the Unix netstat command.

About this task

The following IPv4 socket information is displayed:

- protocol type: TCP/UDP
- number of bytes in receive/send buffers. The Recv-Q and Send-Q counters display a value different from 0 mostly during data transfer.
- local and foreign addresses
- local and foreign ports, appended to the IP adresses
- socket state: CLOSED, LISTEN, SYN_SENT, SYN_RCVD, ESTABLISHED, CLOSE_WAIT, FIN_WAIT_1, CLOSING, LAST_ACK, FIN_WAIT_2, TIME_WAIT
- service type: SSH, TELNET, HTTP, HTTPS, SNMP

Recv-Q/Send-Q counters will display a value different from 0 mostly during data transfer.

Local and foreign protocol ports are appended to the IP addresses.

Foreign IP and port are 0.0.0.0.0 for opened sockets. Only TCP entries have a value in the State column.

The second part of the table (Proto/Port/Service) displays the active services on the device.

The command is available in standalone and stack mode. In stack mode the command is available on base and non-base units and the information displayed is obtained from the base unit.

Procedure

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

```
show ip netstat [tcp | udp]
```

Example

```
5650TD-PWR>show ip netstat

Proto Recv-Q Send-Q Local Address          Foreign Address        State
----- ------ ------ --------------------- ---------------------- -------------
TCP        0      0 10.100.200.90.23      10.100.200.15.33114    ESTABLISHED
TCP        0      0 0.0.0.0.80            0.0.0.0.0              LISTEN
TCP        0      0 0.0.0.0.23            0.0.0.0.0              LISTEN
UDP        0      0 10.100.200.90.3490    0.0.0.0.0
UDP        0      0. 0.0.0.0.161          0.0.0.0.0
-------------------------------------------------------------------------------
Proto Port  Service
----- ----- -------
TCP   23    TELNET
TCP   80    HTTP
UDP   161   SNMP
```


Comments? infodev@avaya.com

Chapter 5: Network monitoring configuration using ACLI

This chapter describes using ACLI to view and configure network monitoring.

Viewing CPU utilization

Use this procedure to view the CPU utilization

Viewing CPU utilization using ACLI

1. Enter Privileged Executive mode.
2. Enter the following command:

```
show cpu-utilization
```

Viewing memory utilization

Use this procedure to view the memory utilization

Viewing memory utilization using ACLI

1. Enter Privileged Executive mode.
2. Enter the following command:

```
show memory-utilization
```

Configuring the system log

This section outlines the ACLI commands used in the configuration and management of the system log.

Displaying the system log

Use this procedure to displays the configuration, and the current contents, of the system event log.

Procedure Steps

Enter the following command Privileged Executive mode:

```
show logging [config] [critical] [serious] [informational]
[sort-reverse]
```

Variable definitions

The following table describes the command variables.

Variable	Value
config	Displays configuration of event logging.
critical	Displays critical log messages.
serious	Displays serious log messages.
informational	Displays informational log messages.
sort-reverse	Displays informational log messages in reverse chronological order (beginning with most recent).
unit <1-8>	Displays log messages for a specific switch in a stack. **Important:** You cannot use this command variable for a standalone switch.

Configuring the system log

Use this procedure to configure the system settings for the system event log.

Procedure Steps

Enter the following command in Global Configuration mode:

Comments? infodev@avaya.com

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

Variable definitions

The following table describes the command variables.

Variable	Value
enable | disable	Enables or disables the event log (default is 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.
volatile <latch | overwrite >	Specifies the options for logging in DRAM.

Disabling the system log

Use this procedure to disable the system event log.

Procedure Steps

Enter the following command in global configuration mode:

```
no logging
```

Setting the system log to default

Use this procedure to default the system event log configuration.

Procedure Steps

Enter the following command in global configuration mode:

```
default logging
```

Clearing the system log

Use this procedure to clear all log messages in DRAM.

Procedure Steps

Enter the following command in global configuration mode:

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

Variable definitions

The following table describes the command variables.

Table 6: clear logging parameters

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

Remote system logging configuration using the ACLI

The following sections describe remote system logging.

Configuring remote system logging

Use this procedure to configure and manage the logging of system messages on a remote server.

Procedure steps

1. Enter the Global Configuration mode.
2. Configure the remote system log by using the following command:

   ```
   logging remote [address <A.B.C.D|WORD>][secondary-address
   <A.B.C.D|WORD][enable][level <critical | informational |
   serious | none>][facility <daemon | local0 | local1 | local2
   | local3 | local4 | local5 | local6 | local7>]
   ```

3. To display the configuration of the system event log, enter the following command:

   ```
   show logging config
   ```

4. To display the current contents of the system event log, enter the following command:

   ```
   show logging [critical | informational | serious | sort-
   reverse | unit <1-8>]
   ```


Comments? infodev@avaya.com

Variable definitions

The following table defines parameters that you can enter with 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*—the IPv4 address of the remote server • *WORD*—the remote host IPv6 address. The value is a character string with a maximum of 45 characters.
`enable`	Enables the system message logging on remote server. **Important:** You must configure either the primary or secondary remote server address before you enable remote logging.
`facility <daemon | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7>`	Configures the remote logging facility used for all messages. If this option is not specified, the default facility is daemon.
`level <critical | informational | serious | none>`	Specifies the remote logging level: • critical—only messages classified as critical are sent to the remote system log server. • serious—only messages classified as serious are sent to the remote system log server. • informational—only messages classified as informational are sent to the remote system log server. • none—no remote 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.

Variable	Value
	• *A.B.C.D*—the IPv4 address of the remote server • *WORD*—the remote host IPv6 address. The value is a character string with a maximum of 45 characters.

Disabling remote system logging

Use this procedure to disable the logging of system messages on a remote server.

Procedure steps

1. Enter the Global Configuration mode.
2. Disable the remote system log by using the following command:

```
no logging remote [address] [secondary-address] [enable]
[facility] [level]
```

Variable definitions

The following table defines parameters that you can enter with the **`no logging remote [address] [secondary-address] [enable] [level]`** command.

Variable	Value
address	Clears the primary remote system log server IP address.
enable	Disables system message logging on the remote server.
facility	Disables logging on the remote logging facility.
level	Clears the remote server logging level.
secondary-address	Clears the secondary remote system log server IP address.

Comments? infodev@avaya.com

Restoring remote system logging to default

Use this procedure to restore the logging of system messages on a remote server to factory defaults.

Procedure steps

1. Enter the Global Configuration mode.
2. Disable the remote system log by using the following command:

```
default logging remote [address][secondary-address][enable]
[facility][level]
```

Variable definitions

The following table defines parameters that you can enter with the **`default logging remote [address] [secondary-address] [enable] [level]`** command.

Variable	Value
address	Restores the primary remote system log server IP address to the factory default (0.0.0.0).
facility	Restores the remote logging facility to default (daemon).
level	Restores the remote server logging level to the factory default (none).
secondary-address	Restores the secondary remote system log server IP address to the factory default (0.0.0.0).

Configuring port mirroring

Port mirroring can be configured with the ACLI commands detailed in this section.

Displaying the port-mirroring configuration

Use this procedure to display the existing port-mirroring configuration.

Procedure Steps

1. Enter Privileged Executive mode.
2. Enter the following command to display the port-mirroring configuration:

```
show port-mirroring
```

Configuring port-mirroring

Use this procedure to set the port-mirroring configuration

Procedure Steps

1. Enter Global Configuration mode.
2. Enter the following command to display the port-mirroring configuration.

```
port-mirroring [1-4][allow-traffic] mode {disable | Xrx
monitor-port <portlist> mirror-ports <portlist> | Xtx
monitor-port <portlist> mirror-ports <portlist> | ManytoOneRx
monitor-port <portlist> mirror-ports <portlist> | ManytoOneTx
monitor-port <portlist> mirror-port-X <portlist> |
ManytoOneRxTx monitor-port <portlist> mirror-port-X
<portlist> | XrxOrXtx monitor-port <portlist> mirror-port-X
<portlist> | XrxOrYtx monitor-port <portlist> mirror-port-X
<portlist> mirror-port-Y <portlist> | XrxYtxmonitor-port
<portlist> mirror-port-X <portlist> mirror-port-Y <portlist>
| XrxYtxOrYrxXtx monitor-port <portlist> mirror-port-X
<portlist> mirror-port-Y <portlist> | Asrc monitor-port
<portlist> mirror-MAC-A <macaddr> | Adst monitor-port
<portlist> mirror-MAC-A <macaddr> | AsrcOrAdst monitor-port
<portlist> mirror-MAC-A <macaddr> | AsrcBdst monitor-port
<portlist> mirror-MAC-A <macaddr> mirror-MAC-B <macaddr> |
AsrcBdstOrBsrcAdst monitor-port <portlist> mirror-MAC-A
<macaddr> mirror-MAC-B <macaddr>} [rspan-vlan <vid>]
```

Variable definitions

The following table outlines the parameters for this command.

Parameter	Description
allow-traffic	Enables bi-direction Monitor Port.
disable	Disables port-mirroring.
monitor-port	Specifies the monitor port.
mirror-port-X	Specifies the mirroring port X.
mirror-port-Y	Specifies the mirroring port Y.

Comments? infodev@avaya.com

Parameter	Description
mirror-MAC-A	Specifies the mirroring MAC address A.
mirror-MAC-B	Specifies the mirroring MAC address B.
portlist	Enter the port numbers.
ManytoOneRx	Many to one port mirroring on ingress packets.
ManytoOneTx	Many to one port mirroring on egress packets.
ManytoOneRxTx	Many to one port mirroring on ingress and egress traffic.
Xrx	Mirror packets received on port X.
Xtx	Mirror packets transmitted on port X.
XrxOrXtx	Mirror packets received or transmitted on port X.
XrxYtx	Mirror packets received on port X and transmitted on port Y. This mode is not recommended for mirroring broadcast and multicast traffic.
XrxYtxOrXtxYrx	Mirror packets received on port X and transmitted on port Y or packets received on port Y and transmitted on port X.
XrxOrYtx	Mirror packets received on port X or transmitted on port Y.
macaddr	Enter the MAC address in format H.H.H.
Asrc	Mirror packets with source MAC address A.
Adst	Mirror packets with destination MAC address A.
AsrcOrAdst	Mirror packets with source or destination MAC address A.
AsrcBdst	Mirror packets with source MAC address A and destination MAC address B.
AsrcBdstOrBsrcAdst	Mirror packets with source MAC address A and destination MAC address B or packets with source MAC address B and destination MAC address A.
rpan-vlan <*vid*>	Specifies the VLAN of the RSPAN source session which is associated to a standard port mirroring session on the source device.

Disabling port-mirroring

Use this procedure to disable port-mirroring

Procedure Steps

1. Enter Global Configuration mode.
2. Enter the following command to disable port-mirroring:

```
no port-mirroring
```

Displaying Many-to-Many port-mirroring

Use this procedure to display Many-to-Many port-mirroring settings

Procedure Steps

1. Enter Privileged Executive mode.
2. Enter the following command:

```
show port-mirroring
```

Configuring Many-to-Many port-mirroring

Use this procedure to configure Many-to-Many port-mirroring

Procedure Steps

1. Enter Global Configuration mode.
2. Enter the following command:

```
port-mirroring <1-4> [allow-traffic] mode {disable | Adst |
Asrc | AsrcBdst | AsrcBdstOrBsrcAdst | AsrcOrAdst |
ManyToOneRx | ManyToOneRxTx | ManyToOneTx | Xrx | XrxOrXtx |
XrxOrYtx | XrxYtx | XrxYtxOrYrxXtx | Xtx}
```

3. Enter the command from preceding step for up to four instances.

Variable definitions

The following table describes the command variables

Variable	Value
allow-traffic	Enables bi-direction Monitor Port.
disable	Disable mirroring.

Comments? infodev@avaya.com

Variable	Value
Adst	Mirror packets with destination MAC address A
Asrc	Mirror packets with source MAC address A.
AsrcBdst	Mirror packets with source MAC address A and destination MAC address B.
AsrcBdstOrBsrcAdst	Mirror packets with source MAC address A and destination MAC address B or packets with source MAC address B and destination MAC address A.
AsrcOrAdst	Mirror packets with source or destination MAC address A.
ManyToOneRx	Mirror many to one port mirroring on ingress packets.
ManyToOneRxTx	Mirror many to one port mirroring on ingress and egress packets.
ManyToOneTx	Mirror many to one port mirroring on egress packets.
Xrx	Mirror packets received on port X.
XrxOrXtx	Mirror packets received on port X and transmitted on port Y.
XrxYtx	Mirror packets received on port X and transmitted on port Y.
XrxYtxOrYrxXtx	Mirror packets received on port X and transmitted on port Y or packets received on port Y and transmitted on port X.
Xtx	Mirror packets received on port X or transmitted on port Y

Disabling Many-to-Many port-mirroring

Procedure Steps

1. Enter Global Configuration mode.
2. Enter on of the following commands to disable a specific instance:

   ```
   port-mirroring [<1-4>] mode disable
   ```

   OR

```
no port-mirroring [<1-4>]
```

3. Enter the following command to disable all instances:

```
no port-mirroring
```

Variable definitions

The following paragraph describes the command variables.

Variable	Definition
<1-4>	The port-mirroring instance.

Displaying RSPAN information

Use this procedure to display the Remote Switch Port Analyzer (RSPAN) information for the switch.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command:

```
show port-mirroring rspan
```

Example

```
5650TD-PWR>enable
5650TD-PWR#show port-mirroring rspan

=========================
RSPAN Source Sessions
=========================
Inst RSPAN VLAN RSPAN MTP
---- ---------- ----------
1    100        1/5
2    100          1/7
3    101        1/9
4    101        2/9

=========================
RSPAN Destination Sessions
=========================
Inst RSPAN VLAN RSPAN MTP
---- ---------- ----------
1    100        2/5
2    101        2/6
3    102        2/7
```


Comments? infodev@avaya.com

```
4    103        2/8
5650TD-PWR#
```

Configuring Remote Switch Port Analyzer (RSPAN)

Use this procedure to configure the Remote Switch Port Analyzer (RSPAN) for the switch.

Before you begin

A dedicated port-based VLAN must be created for the RSPAN VLAN on all involved devices. You can use the `vlan create <vid> type port remote-span` command to create a new VLAN, or `vlan remote-span <vid>` to enable an existing port-based VLAN as an RSPAN VLAN. Use the `show vlan remote-span` command to display RSPAN VLANs.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [no] port-mirroring rspan <1-4> [destination-port <port>]
   [vlan <vid>]
   ```

3. To display the RSPAN settings, enter the following command:

   ```
   show port-mirroring rspan
   ```

Variable definitions

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

Variable	Value
<1–4>	Specifies the RSPAN instance number.
destination-port<*port*>	Specifies the RSPAN destination port.
vlan<*vid*>	Specifies the VLAN of an RSPAN destination session configured on the destination device.
no	Erases RSPAN settings.

Comments? infodev@avaya.com

Chapter 6: RMON configuration using ACLI

Configuring RMON with the ACLI

This section describes the ACLI commands used to configure and manage RMON.

Viewing RMON alarms

Use the following procedure to view RMON alarms.

Procedure Steps

1. Enter Privileged Executive mode.
2. Use the following command to display information about RMON alarms:

```
show rmon alarm
```

Viewing RMON events

Use the following procedure to display information regarding RMON events.

Procedure Steps

1. Enter Privileged Executive mode.
2. Enter the following command:

```
show rmon event
```

Viewing RMON history

Use this procedure to display information regarding the configuration of RMON history.

Procedure Steps

1. Enter Privileged Executive mode.
2. Enter the following command:

```
show rmon history [<port>]
```

Variable Definitions

The following table describes the command variables.

Variable	Definition
<port>	The specified port number for which RMON history settings is displayed.

Viewing RMON statistics

Use the following procedure to display information regarding the configuration of RMON statistics.

Procedure Steps

1. Enter Privileged Executive mode.
2. Enter the following command:

```
show rmon stats
```

Setting RMON alarms

Use the following procedure to set RMON alarms.

Procedure Steps

1. Enter Global Configuration mode.
2. 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 command variables.

Parameter	Description
<1-65535>	Unique index for the alarm entry.

Comments? infodev@avaya.com

Parameter	Description
<WORD>	The MIB object to be monitored. This object identifier can be an English name.
<1-2147483647>	The sampling interval, in seconds.
absolute	Use absolute values (value of the MIB object is compared directly with thresholds).
delta	Use delta values (change in the value of the MIB object between samples is compared with thresholds).
rising-threshold <-2147483648-2147483647 > [<1-65535>]	The first integer value is the rising threshold value. The optional second integer specifies the event entry to be triggered after the rising threshold is crossed. If omitted, or if an invalid event entry is referenced, no event is triggered.
falling-threshold <-2147483648-2147483647 > [<1-65535>]	The first integer value is the falling threshold value. The optional second integer specifies the event entry to be triggered after the falling threshold is crossed. If omitted, or if an invalid event entry is referenced, no event is triggered.
[owner <LINE>]	Specify an owner string to identify the alarm entry.

Deleting RMON alarm table entries

Use the following procedure to delete RMON alarm table entries.

Procedure Steps

1. Enter Global Configuration mode.
2. Enter the following command:

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

Variable definitions

The following table describes the command parameters.

Variable	Definition
[<1-65535>]	The number assigned to the alarm. If no number is selected, all RMON alarm table entries are deleted.

Configuring RMON event log and traps

Use the following procedure to configure RMON event log and trap settings.

Procedure Steps

1. Enter Global Configuration mode.
2. Enter the following command:

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

Variable definitions

The following table describes the command parameters.

Parameter	Description
<1-65535>	Unique index for the event entry.
[log]	Record events in the log table.
[trap]	Generate SNMP trap messages for events.
[description <LINE>]	Specify a textual description for the event.
[owner <LINE>]	Specify an owner string to identify the event entry.

Deleting RMON event table entries

Use the following procedure to clear entries in the table.

Procedure Steps

1. Enter Global Configuration mode.
2. Enter the following command to delete the entries:

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

Variable definitions

The following table describes the command parameters.

Comments? infodev@avaya.com

Variable	Definition
[<1-65535>]	Unique identifier of the event. If not given, all table entries are deleted.

Configuring RMON history

Use the following procedure to configure RMON history settings.

Procedure Steps

1. Enter Global Configuration mode.
2. Enter the following command to configure the RMON history:

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

The **`rmon history`** command is executed in the Global Configuration command mode.

Variable definitions

The following table describes the command variables

Table 7: rmon history parameters

Parameter	Description
<1-65535>	Unique index for the history entry.
<LINE>	Specify the port number to be monitored.
<1-65535>	The number of history buckets (records) to keep.
<1-3600>	The sampling rate (how often a history sample is collected).
[owner <LINE>]	Specify an owner string to identify the history entry.

Deleting RMON history table entries

Use this procedure to delete RMON history table entries.

Procedure Steps

1. Enter Global Configuration mode.
2. Enter the following command to delete the entries:

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

Variable definitions

The following table describes the command parameters.

Variable	Definition
[<1-65535>]	Unique identifier of the event. If not given, all table entries are deleted.

Configuring RMON statistics

Use this procedure to configure RMON statistics settings.

Procedure Steps

1. Enter Global Configuration mode.
2. Enter the following command to configure RMON statistics:

```
rmon stats <1-65535> <LINE> [owner <LINE>]
```

Variable definitions

The following table describes the command variables.

Parameter	Description
<1-65535>	Unique index for the stats entry.
[owner <LINE>]	Specify an owner string to identify the stats entry.

Disabling RMON statistics

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

Procedure Steps

1. Enter Global Configuration mode.
2. Enter the following command to disable RMON statistics:

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


Comments? infodev@avaya.com

Variable definitions

The following table describes the command parameters.

Variable	Definition
<1-65535>	Unique index for the statistics entry. If omitted, all statistics are disabled.

Comments? infodev@avaya.com

Chapter 7: IPFIX Configuration using ACLI

This section describes the commands used in the configuration and management of IP Flow Information Export (IPFIX) using the ACLI.

Configuring IPFIX collectors

The **`ip ipfix collector`** command is used to configure IPFIX collectors. IPFIX collectors are used to collect and analyze data exported from an IPFIX compliant switch. In Software Release 5.0, the only external collector supported is **NetQOS**. At this time, up to two collectors can be supported.

IPFIX data is exported from the switch in *Netflow version 9* format. Data is exported using UDP port 9995.

IPFIX data is not load balanced when two collectors are in use. Identical information is sent to both collectors.

Use the following procedure to configure the IPFIX collectors.

Procedure Steps

1. Enter Global Configuration mode.
2. Use the following command to configure the IPFIX collector:

```
ip ipfix collector <collector_ip_address>
```

The **`ip ipfix collector`** command is executed in the Global Configuration mode.

Variable definitions

The following table describes the parameters for this command.

Parameter	Description
<collector_ip_address>	The IP address of the collector.

Enabling IPFIX globally

Use the following procedure to globally enable IPFIX on the switch.

Procedure Steps

1. Enter Global Configuration mode.
2. Use the following command to enable IPFIX on the switch:

```
ip ipfix enable
```

Configuring unit specific IPFIX

Use the following command to configure unit specific IPFIX parameters.

Procedure Steps

1. Enter Global Configuration mode.
2. Use the following command to enable IPFIX on the switch:

```
ip ipfix slot <unit_number> [aging-interval <aging_interval>]
[export-interval <export_interval>] [exporter-enable]
[template-refresh-interval <template_refresh_interval>]
[template-refresh-packets <template_refresh_packets>]
```

Variable definitions

The parameters of this command are described in the following table.

Parameter	Description
<unit_number>	The unit number of the collector. Currently up to two collectors are supported so the values 1 or 2 are valid.
<aging_interval>	The IPFIX aging interval. This value is in seconds from 0 to 2147400.
<export_interval>	The IPFIX export interval. This interval is the value at which IPFIX data is exported in seconds from 10 to 3600.
<template_refresh_interval>	The IPFIX template refresh interval. This value is in seconds from 300 to 3600.

Comments? infodev@avaya.com

Parameter	Description
<template_refresh_packets>	The IPFIX template refresh packet setting. This value is the number of packets from 10000 - 100000.

Enabling IPFIX on the interface

Use the following procedure to enable IPFIX on the interface.

Procedure Steps

1. Enter Interface Configuration mode.
2. Use the following command to enable IPFIX on the interface:

```
ip ipfix enable
```

Enabling IPFIX export through ports

Use the following procedure to enable the ports exporting data through IPFIX.

Procedure Steps

1. Enter Interface Configuration mode.
2. Use the following command to enable IPFIX on the interface:

```
ip ipfix port <port_list>
```

Variable definitions

The following table describes the command parameters

Variable	Definition
port-list	Single or comma-separated list of ports.

Deleting the IPFIX information for a port

Use the following procedure to delete the collected IPFIX information for a port.

Procedure Steps

1. Enter Privileged Executive mode.
2. Use the following command to delete the collected IPFIX information for the port or ports:

```
ip ipfix flush port <port_list> [export-and-flush]
```

Variable definitions

The following table describes the command parameters.

Variable	Definition
port-list	Single or comma-separated list of ports.
export-and-flush	Export data to a collector before it is deleted.

Viewing the IPFIX table

Use the following procedure to display IPFIX data collected from the switch.

Procedure Steps

1. Enter Privileged Executive mode.
2. Use the following command view the IPFIX data:

```
show ip ipfix table <unit_number> sort-by <sort_by> sort-
order <sort_order> display <num_entries>
```

Variable definitions

The following table describes the command parameters.

Variable	Definition
<unit_number>	The unit number of the collector. Currently up to two collectors are supported so the values 1 or 2 are valid.
<sort_by>	The value on which the data is sorted. Valid options are: • byte-count • dest-addr

Comments? infodev@avaya.com

Variable	Definition
	• first-pkt-time • last-pkt-time • pkt-count • port • protocol • source-addr • TCP-UDP-dest-port • TCP-UDP-src-port • TOS
<sort_order>	The order in which the data is sorted. Valid options are ascending and descending.
<num_entries>	The number of data rows to display. Valid options are: • all • top-10 • top-25 • top-50 • top-100 • top-200

Comments? infodev@avaya.com

Chapter 8: System diagnostics and statistics using Enterprise Device Manager

This chapter describes the procedures you can use to perform system diagnostics and gather statistics using Enterprise Device Manager (EDM).

Configuring Stack Monitor using EDM

Use the following procedure to configure Stack Monitor using EDM.

Procedure Steps

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

Variable definitions

The following table describes the fields of Stack Monitor tab.

Field	Description
StackErrorNotificationEnabled	Enables or disables the Stack Monitoring feature.
ExpectedStackSize	Specifies the size of the stack to monitor. Valid range is 2–8. Default value is 2.

Field	Description
StackErrorNotificationInterval	Specifies the time interval between traps, in seconds. Valid range is 30–300 seconds. Default value is 60.
StackRebootUnitOnFailure	Enables or disables the rebooting stack units on failure.
StackRetryCount	Sets the retry count for the stack.

Viewing stack health using EDM

Use this procedure to display stack health information.

Procedure steps

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

Variable definitions

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

Variable	Value
Switch Units Found	Indicates the number of switch units in the stack.
Stack Health Check	Indicates the stack health.
Stack Diagnosis	Indicates the stack mode.

Viewing power supply information

Use this procedure to display the operating status of switch power supplies.

Comments? infodev@avaya.com

Procedure

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

Power Supply field descriptions

The following table describes the fields on the **Power Supply** tab.

Name	Description
Description	Indicates the chassis number, power supply number, and the type of power supply.
OperState	• **other**: Some other state • **notAvail**: State not available • **removed**: Component was removed • **disabled**:Operation disabled • **normal**: State is in normal operation • **resetInProg**: There is a reset in progress • **testing**: System is doing a self test • **warning**: System is operating at a warning level • **nonFatalErr**: System is operating at error level • **fatalErr**: A fatal error stopped operation • **notConfig**: A module needs to be configured. The allowable values are determined by the component type.

Viewing switch fan information

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

Procedure

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

Variable definitions

The following table describes the fields of 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

Viewing switch temperature

Use the following procedure to display switch temperature information.

Procedure

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

Comments? infodev@avaya.com

Variable definitions

The following tables describes the fields of the **Temperature** tab.

Name	Description
Unit	Indicates the switch unit number in a stack. For a standalone switch, the default value is 1.
Temperature	Indicates the switch unit operating temperature.

Comments? infodev@avaya.com

Chapter 9: Network monitoring configuration using Enterprise Device Manager

This chapter describes the procedures you can use to perform network monitoring configuration using Enterprise Device Manager (EDM).

CPU and memory utilization using EDM

Use the following procedure to view CPU and memory utilization.

Prerequisites

- Open one of the supported browsers.
- Enter the IP address of the switch to open an EDM session.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Chassis**.
4. On the work area, click the **CPU/Memory Utilization** tab.
5. On the toolbar, click the **Refresh** button to update the data.

Variable definitions

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

Field	Description
Unit	Indicates the unit.
Last10Seconds	Indicates the CPU usage, in percentage, for the last 10 seconds.
Last1Minute	Indicates the CPU usage, in percentage, for the last minute.
Last10Minutes	Indicates the CPU usage, in percentage, for the last 10 minutes.
Last1Hour	Indicates the CPU usage, in percentage, for the last hour.
Last24Hours	Indicates the CPU usage, in percentage, for the last 24 hours.
TotalCPUUsage	Indicates the memory usage in megabytes.
MemoryTotalMB	Indicates the total memory present, in megabytes, on the unit.
MemoryAvailableMB	Indicates the remaining memory on the unit.
MemoryUsedMB	Indicates the memory being used on the unit.

Switch stack information management

Use the information in the following sections to display and edit switch stack information.

Viewing stack information

Use this procedure to display information about the operating status of stack switches.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, click **Switch/Stack**.
4. In the work area, click the **Stack Info** tab.

Comments? infodev@avaya.com

Stack Info field descriptions

The following table outlines the parameters for the **Stack Info** tab.

Name	Description
Indx	Indicates the line number for stack info. This is a read-only cell.
Descr	Describes the component or subcomponent. If not available, the value is a zero length string. This is a read-only cell.
Location	Indicates the geographic location of a component in a system modeled as a chassis, but possibly physically implemented with geographically separate devices connected to exchange management information. Chassis modeled in this manner are sometimes referred to as virtual chassis. An example value is: **4th flr wiring closet in blg A**. **Important:** This field applies only to components that are in either the Board or Unit groups. If the information is unavailable, for example, the chassis is not modeling a virtual chassis or component is not in a Board or Unit group, the value is a zero-length string. If this field is applicable and is not assigned a value through a SNMP SET PDU when the row is created, the value defaults to the value of the object s5ChasComSerNum.
LstChng	Indicates the value of sysUpTime when it was detected that the component or sub-component was added to the chassis. If this action has not occurred since the cold or warm start of the agent, the value is zero.
AdminState	Specifies the state of the component or subcomponent. • **enable**: enables operation • **reset**: resets component

Name	Description
OperState	Indicates the current operational state of the component. The possible values are • **other**: another state • **notAvail**: state not available • **removed**: component removed • **disabled**: operation disabled • **normal**: normal operation • **resetInProg**: reset in progress • **testing**: performing a self test • **warning**: operating at warning level • **nonFatalErr**: operating at error level • **fatalErr**: error stopped operation
Ver	Indicates the version number of the component or subcomponent. If not available, the value is a zero-length string.
SerNum	Indicates the serial number of the component or subcomponent. If not available, the value is a zero-length string.
BaseNumPorts	Indicates the number of base ports of the component or subcomponent.
TotalNumPorts	Indicates the number of ports of the component or subcomponent.
IpAddress	Indicates the IP address of the component or subcomponent.
RunningSoftwareVer	Indicates the software version running on the switch.

Editing stack information

Use this procedure to change the information about the switch units in the stack.

Procedure

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

Comments? infodev@avaya.com

4. In the work area, click the **Stack info** tab.
5. To select a switch unit for which to edit information, click a switch row.
6. In the row, double-click the cell in the **Location** column.
7. Type a location.
8. In the row, double-click the cell in the **AdminState** column.
9. Select a value from the list.
10. On the toolbar, click **Apply**.

Stack Info field descriptions

The following table outlines the parameters for the **Stack Info** tab.

Name	Description
Indx	Indicates the line number for stack info. This is a read-only cell.
Descr	Describes the component or subcomponent. If not available, the value is a zero length string. This is a read-only cell.
Location	Specifies the geographic location of a component in a system modeled as a chassis, but possibly physically implemented with geographically separate devices connected to exchange management information. Chassis modeled in this manner are sometimes referred to as virtual chassis. An example value is: **4th flr wiring closet in blg A**. **Important:** This field applies only to components that are in either the Board or Unit groups. If the information is unavailable, for example, the chassis is not modeling a virtual chassis or component is not in a Board or Unit group, the value is a zero-length string. If this field is applicable and is not assigned a value through a SNMP SET PDU when the row is created, the value defaults to the value of the object s5ChasComSerNum.

Name	Description
LstChng	Indicates the value of sysUpTime when it was detected that the component or sub-component was added to the chassis. If this action has not occurred since the cold or warm start of the agent, the value is zero. This is a read-only cell.
AdminState	Specifies the state of the component or subcomponent. • **enable**: enables operation • **reset**: resets component
OperState	Indicates the current operational state of the component. This is a read-only cell. Values include: • **other**: another state • **notAvail**: state not available • **removed**: component removed • **disabled**: operation disabled • **normal**: normal operation • **resetInProg**: reset in progress • **testing**: performing a self test • **warning**: operating at warning level • **nonFatalErr**: operating at error level • **fatalErr**: error stopped operation The component type determines the allowable (and meaningful) values.
Ver	Indicates the version number of the component or subcomponent. If not available, the value is a zero-length string. This is a read-only cell.
SerNum	Indicates the serial number of the component or subcomponent. If not available, the value is a zero-length string. This is a read-only cell.
BaseNumPorts	Indicates the number of base ports of the component or subcomponent. This is a read-only cell.
TotalNumPorts	Indicates the number of ports of the component or subcomponent. This is a read-only cell.

Comments? infodev@avaya.com

Name	Description
IpAddress	Indicates the IP address of the component or subcomponent. This is a read-only cell.
RunningSoftwareVer	Indicates the software version running on the switch. This is a read-only cell.

Viewing pluggable ports

Use this procedure to display pluggable port information.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, click **Switch/Stack**.
4. In the work area, click the **Stack info** tab to display the current stack information.
5. To select a switch unit for which to display information, click a switch row.
6. On the toolbar, click **Pluggable Ports**.

Pluggable Ports field descriptions

The following table describes the fields of the **Pluggable Ports** tab.

Name	Description
Unit	Identifies the unit number.
Port	Identifies the number of the pluggable port.
PortType	Identifies the type of the pluggable port.
VendorName	Identifies the vendor's name.
VendorOUI	Identifies the Vendor Organizationally Unique Identifier
VendorPartNo	Identifies the vendor's part number.
VendorRevision	Identifies the vendor's revision.
VendorSerial	Identifies the vendor's serial number.
HWOptions	Identifies the hardware options.

Name	Description
DateCode	Identifies the date code.
VendorData	Identifies vendor data.
OrderCode	Identifies the order code.

Configuring the system log using EDM

Use the following procedure to configure the system log.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **System Log**.
4. In the **System Log Settings** tab, configure the required parameters.
5. On the toolbar, click **Apply**.

Variable definitions

The following table describes the fields in the **System Log Settings** tab.

Field	Description
Operation	Turns the system log on or off.
BufferFullAction	Specifies whether the system log overwrites itself or discontinues the storage of messages when the buffer is full.
Volatile - CurSize	Shows the current number of messages stored in volatile memory.
Volatile - SaveTargets	Indicates the severity of system messages to save. Available options are: • critical • critical/serious • critical/serious/inform • none

Comments? infodev@avaya.com

Field	Description
	Default value is critical/serious/inform.
non - Volatile - CurSize	Shows the current number of messages stored in non-volatile memory.
non-Volatile - SaveTargets	Indicates the severity of system messages to save. Available options are: • critical • critical/serious • none Default value is critical/serious.
ClearMessageBuffers	Selects the sections of the system log to delete. Available options are: • volCritical • volSerious • volInformational • nonVolCritical • nonVolSerious
CLI Audit Log	Enables or disables CLI audit logging to a reserved Flash area.

Viewing system logs using EDM

Use the following procedure to display system log information.

Procedure steps

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

Variable definitions

Use the data in the following table to help you understand the system log display.

Variable	Value
OrigUnitNumber	Indicates the slot or unit number of the originator of a log message.
MsgTime	Indicates the time (in one hundredths of a second) between system initialization and the appearance of a log message in the system log.
MsgIndex	Indicates a sequential number the system assigns to a log message when it enters the system log.
MsgSrc	Indicates whether a log message was loaded from non-volatile memory at system initialization or was generated since system initialization.
MsgType	Indicates the type of message: Critical, Serious, or Information.
MsgString	Indicates the log message originator and the reason the log message was generated.

Viewing system log settings

To view the System Log Settings tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **System Log**.
4. Select the **System Log Settings** tab.

The following table outlines the parameters of the **System Log Settings** tab.

Table 8: Variable definitions

Variable	Value
Operation	Enables (on) or disables (off) the system log.

Comments? infodev@avaya.com

Variable	Value
BufferFullAction	Specifies the action for the system to take when the buffer space allocated for system log messages is exhausted. • overwrite—previously logged messages are overwritten • latch—halts the saving of system log messages until overwrite is selected, or buffer space is made available by other means (for example, clearing the buffer).
CurSize	Indicates the number of messages currently stored in memory.
SaveTargets	Specifies the type of system messages to save in memory. • critical—only messages classified as critical are saved in memory • critical/serious—only messages classified as critical and serious are saved in memory • critical/serious/inform—only messages classified as critical, serious, and informational are saved in memory • none—no system log messages are saved in memory
ClearMessageBuffers	Specifies the types of system log messages to delete from volatile and non-volatile memory. • volCritical—only messages classified as critical are deleted from volatile memory • volSerious—only messages classified as serious are deleted from volatile memory • volInformational—only messages classified as informational are deleted from volatile memory • nonVolCritical—only messages classified as critical are deleted from non-volatile memory • nonVolSerious—only messages classified as serious are deleted from non-volatile memory
Enable	Enable or disable CLI audit logs from being stored in a reserved Flash area.

Remote system logging using EDM

The following sections describes remote system logging procedures using EDM.

Viewing remote system log properties

To view the Remote System Log tab:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **System Log**.
4. Select the **Remote System Log** tab.

The following table outlines the parameters of the **Remote System Log** tab.

Table 9: Variable definitions

Variable	Value
RemoteSyslogAddressType	Specifies the type of IP address of the remote system log server.
RemoteSyslogAddress	Specifies the IP address of the remote system log server when sending system log messages.
SecondarySyslogAddressType	Specifies the type of IP address of the secondary remote system log server.
SecondarySyslogAddress	Specifies the IP address of the secondary remote system log server when sending system log messages.
Enabled	Enables or disables the remote logging of system messages.
SaveTargets	Specifies the type of system messages to send to the remote system log server. • 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
Facility	Specifies the remote logging facility. • Daemon • Local0 • Local1

Comments? infodev@avaya.com

Variable	Value
	• Local2 • Local3 • Local4 • Local5 • Local6 • Local7 DEFAULT: Daemon

Configuring remote system logging using EDM

Use this procedure to configure and manage the logging of system messages on a secondary, remote syslog server.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **System Log**.
4. In the work area, click the **Remote System Log** tab.
5. In the **RemoteSyslogAddressType** section, click the type of IP address of the remote system log server.
6. In the **RemoteSyslogAddress** box, type the IP address of the remote system log server.
7. In the **SecondarySyslogAddressType** section, click the type of IP address of the remote system log server.
8. In the **SecondarySyslogAddress** box, type the IP address of the remote system log server.
9. Click the **Enabled** box to enable remote system logging.

   OR

   Click the **Enabled** box to disable remote system logging.
10. In the **SaveTargets** section, click the type of system messages.
11. On the tool bar, click **Apply**.

Variable definitions

Use the data in the following table to help you configure the remote system log.

Variable	Value
RemoteSyslogAddressType	Specifies the type of IP address of the remote system log server.
RemoteSyslogAddress	Specifies the IP address of the remote system log server to which to send system log messages.
SecondarySyslogAddressType	Specifies the type of IP address of the secondary remote system log server.
SecondarySyslogAddress	Specifies the IP address of the secondary remote system log server to send system log messages to.
Enabled	Enables or disables the remote logging of system messages.
SaveTargets	Specifies the type of system messages to send to the remote system log server. • 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
Faciltiy	Specifies the remote logging facility. • Daemon • Local0 • Local1 • Local2 • Local3 • Local4 • Local5

Comments? infodev@avaya.com

Variable	Value
	• Local6 • Local7 DEFAULT: Daemon

EDM MIB Web page

Use the information in this section to use the EDM MIB Web page to monitor network SNMP characteristics.

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

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

Procedure steps

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

   The result of the request appears in the Result area of the window. If the request is unsuccessful, a description of the received error appears.
5. Click **Get Next** to retrieve the information of the next object in the MIB.
6. Repeat step 3 as required.

Using the EDM MIB Web page for SNMP walk

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

Perform this procedure to request the result of MIB Walk.

Procedure steps

1. From the navigation tree, double-click **Administration**.
2. In the Administration tree, double-click **MIB Web Page**.

3. In the **MIB Name/ OID** box, enter the object name or OID.
4. Click **Walk**.

   The result of the request appears in the Result area. If the request is unsuccessful, a description of the received error appears.

Port Mirroring using EDM

The following sections describe Port Mirroring.

Viewing Port Mirroring using EDM

View Port Mirroring to troubleshoot the network.

Procedure steps

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

Variable definitions

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

Variable	Value
Instance	Specifies the numerical assignment of the port mirroring.
Port Mode	Specifies the port monitoring mode.
Monitor Port	Identifies the monitoring port.
PortListX	Identifies the ports monitored for XrX/Xtx, and manytoOne related mode.
PortListY	Identifies the ports monitored for Yrx/Ytx related mode.
MacAddressA	Specifies the MAC address of the monitored port using Sarc/ Adst related mode.
MacAddressB	Specifies the MAC address of the monitored port using Bsrc/ Bdst related mode.
AllowTraffic	Indicates whether bi-directional mirroring traffic is enabled.

Comments? infodev@avaya.com

Variable	Value
RspanVlan	Indicates the RSPAN VLAN ID

Configuring Port Mirroring using EDM

Configure Port Mirroring to troubleshoot the network.

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, double-click **Port Mirrors**.
4. In the work area, click **Insert**
5. In the **Instance** box, type an instance number.
6. In the **PortMode** section, click a mode.
7. Click the **MonitorPort** ellipsis (**...**).
8. In the **MonitorPort** list, click a monitor port.
9. Click **Ok**.
10. If the PortMode is Xrx, Xtx,or both, or manytoOne releated modes, click the **PortListX** ellipsis (**...**).
11. In the **PortListX** list, click a port, ports, or **All** to add to the list.
12. Click **Ok**.
13. If the PortMode is Yrx, Ytx, or both related modes, click the **PortListY** ellipsis (**...**) .
14. In the **PortListY**, click a port, ports, or **All** to add to the list.
15. Click **Ok**.
16. If the PortMode is Asrc, Adst, or both related modes, in the **MacAddressA**, type an address.
17. If the PortMode is Bsrc, Bdst, or both related modes, in the **MacAddressA**, type an address.
18. To enable bi-directional traffic, click the **AllowTraffic** box.
19. Click the **RspanVlan** ellipsis (**...**).
20. In the **RspanVLan** list, click a VLAN ID.

21. Click **Ok**.
22. Click **Insert**.

Variable definitions

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

Variable	Value
Instance	Indicates the Port Mirroring instance number.
PortMode	Indicates the supported Port Mirroring modes. The modes are: • Adst—Mirror packets with destination MAC address A. • Asrc—Mirror packets with source MAC address A. • AsrcBdst—Mirror packets with source MAC address A and destination MAC address B. • AsrcBdstOrBsrcAdst—Mirror packets with source MAC address A and destination MAC address B or packets with source MAC address B and destination MAC address A. • AsrcOrAdst—Mirror packets with source or destination MAC address A. • manytoOneRx—Many to one port mirroring on ingress packets. • manytoOneRxTx—Many to one port mirroring on ingress and egress traffic. • manytoOneTx—Many to one port mirroring on egress packets. • Xrx—Mirror packets received on port X. • XrxOrXtx—Mirror packets received or transmitted on port X. • XrxOrYtx—Mirror packets received on port X or transmitted on port Y. • XrxYtx—Mirror packets received on port X and transmitted on port Y. This mode is not recommended for mirroring broadcast and multicast traffic. • XrxYtxOrXtxYrx—Mirror packets received on port X and transmitted on port Y or

Comments? infodev@avaya.com

Variable	Value
	packets received on port Y and transmitted on port X. • Xtx—Mirror packets transmitted on port X. The default value is Disabled.
MonitorPort	Specifies 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.
PortListY	Indicates the switch port to be monitored by the designated monitor port. This port is monitored according to the value Y in the Monitoring Mode field.
MacAddressA	Specifies the mirroring MAC address A.
MacAddressB	Specifies the mirroring MAC address B.
AllowTraffic	Indicates whether bi-directional traffic is enabled.
RspanVlan	Indicates the RSPAN VLAN ID.

Configuring RSPAN

Use this procedure to Configure Remote Switch Port Analyzer (RSPAN) for the switch.

Before you begin

A dedicated port-based VLAN must be created for the RSPAN VLAN.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the Diagnostics tree, click **Port Mirrors**.
4. Select the **RSPAN** tab.
5. In the work area, click **Insert**.
6. In the **Instance** box, type an instance number.
7. Click the **Destination Port** ellipsis (...).

8. In the **Destination Port** list, click a destination port..
9. Click **Ok**.
10. Click the **RspanVlan** ellipsis (...).
11. In the **RspanVlan** list, click a VLAN ID.
12. Click **Ok**.
13. Click **Insert**.

Creating a graph using EDM

Several screens in the EDM provide a means to view and make use of statistical information gathered by the switch.

Use the following procedure to turn this statistical information in either a bar, line, area, or pie graph.

Procedure steps

1. Open a window that provides graphing capabilities.
2. Click the desired tab.
3. Select the information that you want to graph.
4. In the toolbar, click the graph button that corresponds to the type of graph you want to create.

Graphing switch chassis data using EDM

Use the following procedure to view switch statistical information in a variety of graphs.

Procedure steps

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the tab you want to view.

Comments? infodev@avaya.com

Graphing the SNMP tab using EDM

Use the following procedure to view read-only statistical information about SNMP traffic in the SNMP tab.

Procedure steps

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **SNMP** tab to view the SNMP statistical information.

Variable definitions

The following table describes the fields of **SNMP** tab.

Field	Description
InPkts	Indicates the total number of messages delivered to the SNMP from the transport service.
OutPkts	Indicates the total number of SNMP messages passed from the SNMP protocol to the transport service.
InTotalReqVars	Indicates the total number of MIB objects retrieved successfully by the SNMP protocol as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
InTotalSetVars	Indicates the total number of MIB objects altered successfully by the SNMP protocol as the result of receiving valid SNMP Set-Request PDUs.
InGetRequests	Indicates the total number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP protocol.
InGetNexts	Indicates the total number of SNMP Get-Next PDUs accepted and processed by the SNMP protocol.
InSetRequests	Indicates the total number of SNMP Set-Request PDUs accepted and processed by the SNMP protocol.
InGetResponses	Indicates the total number of SNMP Get-Response PDUs accepted and processed by the SNMP protocol.
OutTraps	Indicates the total number of SNMP Trap PDUs generated by the SNMP protocol.

Field	Description
OutTooBigs	Indicates the total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is tooBig.
OutNoSuchNames	Indicates the total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is noSuchName.
OutBadValues	Indicates the total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is badValue.
OutGenErrs	Indicates the total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is genErr.
InBadVersions	Indicates the total number of SNMP messages delivered to the SNMP protocol for an unsupported SNMP version.
InBadCommunityNames	Indicates the total number of SNMP messages delivered to the SNMP protocol that used an unknown SNMP community name.
InBadCommunityUses	Indicates the total number of SNMP messages delivered to the SNMP protocol that represented an SNMP operation not allowed by the SNMP community named in the message.
InASNParseErrs	Indicates the total number of ASN.1 or BER errors encountered by the SNMP protocol after decoding received SNMP messages.
InTooBigs	Indicates the total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is tooBig.
InNoSuchNames	Indicates the total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is noSuchName.
InBadValues	Indicates the total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is badValue.
InReadOnlys	Indicates the total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is readOnly. This error is a protocol error to generate an SNMP PDU containing the value "readOnly" in the error-status field. This object is provided to detect incorrect implementations of the SNMP.
InGenErrs	Indicates the total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is genErr.

Comments? infodev@avaya.com

Graphing the IP tab using EDM

Use this procedure to graph information about the IP packets that are interfaced with the switch

Procedure steps

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **IP** tab to view the SNMP statistical information.

Variable definitions

The following table outlines the fields of **IP** tab.

Field	Description
InReceives	Indicates the total number of input datagrams received from interfaces, including those received in error.
InHdrErrors	Indicates 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	Indicates 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	Indicates 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 that were Source-Routed by way of this address and had successful Source-Route option processing.
InUnknownProtos	Indicates the number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InDiscards	Indicates the number of input IP datagrams for which no problems were encountered to prevent their continued processing but that were discarded (for example, for lack of buffer space). This counter

Field	Description
	does not include any datagrams discarded while awaiting reassembly.
InDelivers	Indicates the total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	Indicates 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	Indicates the number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that were discarded (for example, for lack of buffer space). This counter will include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
OutNoRoutes	Indicates the number of IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in ipForwDatagrams that meet this no-route criterion. This includes any datagrams a host cannot route because all of its default gateways are down.
FragOKs	Indicates the number of IP datagrams that have been successfully fragmented at this entity.
FragFails	Indicates the number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, for example, because their Don't Fragment flag was set.
FragCreates	Indicates the number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
ReasmReqds	Indicates the number of IP fragments received that needed to be reassembled at this entity.
ReasmOKs	Indicates the number of IP datagrams successfully reassembled.
ReasmFails	Indicates the number of failures detected by the IP reassembly algorithm. This is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.

Graphing the ICMP In tab using EDM

Use the following procedure to view read-only information about inbound ICMP messages.

Comments? infodev@avaya.com

Procedure steps

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **ICMP In** tab to view the information about inbound ICMP messages.

Variable definitions

The following table describes the fields of **ICMP In** tab.

Field	Description
SrcQuenchs	Indicates the number of ICMP Source Quench messages received.
Redirects	Indicates the number of ICMP Redirect messages received.
Echos	Indicates the number of ICMP Echo (request) messages received.
EchoReps	Indicates the number of ICMP Echo Reply messages received.
Timestamps	Indicates the number of ICMP Timestamp (request) messages received.
TimestampReps	Indicates the number of ICMP Timestamp Reply messages received.
AddrMasks	Indicates the number of ICMP Address Mask Request messages received.
AddrMaskReps	Indicates the number of ICMP Address Mask Reply messages received.
ParmProbs	Indicates the number of ICMP Parameter Problem messages received.
DestUnreachs	Indicates the number of ICMP Destination Unreachable messages received.
TimeExcds	Indicates the number of ICMP Time Exceeded messages received.

Graphing the ICMP Out tab using EDM

Use the following procedure to view read-only information about outbound ICMP messages.

Procedure steps

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **ICMP Out** tab to view the information about outbound ICMP messages.

Variable definitions

The following table describes the fields of **ICMP Out** tab.

Field	Description
SrcQuenchs	Indicates the number of ICMP Source Quench messages sent.
Redirects	Indicates the number of ICMP Redirect messages received. For a host, this object will always be zero, because hosts do not send redirects.
Echos	Indicates the number of ICMP Echo (request) messages sent.
EchoReps	Indicates the number of ICMP Echo Reply messages sent.
Timestamps	Indicates the number of ICMP Timestamp (request) messages sent.
TimestampReps	Indicates the number of ICMP Timestamp Reply messages sent.
AddrMasks	Indicates the number of ICMP Address Mask Request messages sent.
AddrMaskReps	Indicates the number of ICMP Address Mask Reply messages sent.
ParmProbs	Indicates the number of ICMP Parameter Problem messages sent.
DestUnreachs	Indicates the number of ICMP Destination Unreachable messages sent.
TimeExcds	Indicates the number of ICMP Time Exceeded messages sent.

Graphing the TCP tab using EDM

Use the following procedure to view read-only information about TCP activity on the switch.

Comments? infodev@avaya.com

Procedure steps

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **TCP** tab to view the information about TCP activity on the switch.

Variable definitions

The following table describes the fields of **TCP** tab.

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

Field	Description
HCInSegs	Indicates 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	Indicates 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.

Graphing the UDP tab using EDM

Use the following procedure to view read-only information about UDP activity on the switch.

Procedure steps

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **UDP** tab to view the information about UDP activity on the switch.

Variable definitions

The following table describes the fields of **UDP** tab.

Field	Description
InDatagrams	Indicates the total number of UDP datagrams delivered to UDP users
NoPorts	Indicates the total number of received UDP datagrams for which there was no application at the destination port.
InErrors	Indicates the number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
OutDatagrams	Indicates the total number of UDP datagrams sent from this entity.
HCInDatagrams	Indicates the number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
HCOutDatagrams	Indicates the number of UDP datagrams sent from this entity, for devices that can transmit more than 1 million UDP datagrams for each second.

Comments? infodev@avaya.com

Field	Description
	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.

Graphing switch port data using EDM

This section describes the procedures you can use to view port statistical information in a variety of graphs.

Use the following procedure to select a port or ports to graph.

Procedure steps

1. In the **Device Physical View**, select one or multiple ports.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the tab you want to view.

Some statistics are only available after a single port is graphed.

Graphing the Interface tab using EDM

Use the following procedure to view read-only information about the selected interfaces.

Procedure steps

1. In the **Device Physical View**, select one or multiple ports.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **Interface** tab to view information about the selected interfaces.

Variable definitions

The following table describes the fields of **Interface** tab.

Field	Description
InOctets	Indicates the total number of octets received on the interface, including framing characters.
OutOctets	Indicates the total number of octets transmitted out of the interface, including framing characters.
InUcastPkts	Indicates the number of packets delivered by this sublayer to a higher sublayer that were not addressed to a multicast or broadcast address at this sublayer.
OutUcastPkts	Indicates the number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast address at this sublayer. This total number includes those packets discarded or unsent.
InNUcastPkts	Indicates the number of packets delivered by this sublayer to a higher (sub)layer, which were addressed to a multicast or broadcast address at this sublayer.
OutNUcastPkts	Indicates the total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent.
InDiscards	Indicates the number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
OutDiscards	Indicates the number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet is 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 could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.
InUnknownProtos	For packet-oriented interfaces, the number of packets received through the interface that were 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 were discarded because of an unknown or unsupported

Comments? infodev@avaya.com

Field	Description
	protocol. For an interface that does not support protocol multiplexing, this counter will always be 0.

Graphing Ethernet Errors tab using EDM

Use the following procedure to view read-only information about port Ethernet error statistics.

Procedure steps

1. In the **Device Physical View**, select one or multiple ports.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **Ethernet Errors** tab to view information about port Ethernet error statistics.

Variable definitions

The following table describes the fields of **Ethernet Errors** tab.

Field	Description
AlignmentErrors	Indicates the count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented after 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	Indicates the 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 after the frameCheckError 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

Field	Description
	the conventions of IEEE 802.3 Layer management, counted exclusively according to the error status presented to the LLC.
InternalMacTransmitErrors	Indicates the 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	Indicates the 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 may represent a count of receive errors on a particular interface that are not otherwise counted.
CarrierSenseErrors	Indicates the number of times that the carrier sense condition was lost or never asserted after attempting to transmit a frame on a 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.
FrameTooLongs	Indicates the 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 after the frameTooLong 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	Indicates the count of times that the SQE TEST ERROR 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

Comments? infodev@avaya.com

Field	Description
	ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
DeferredTransmissions	Indicates the 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	Indicates the 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	Indicates the count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	Indicates 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	Indicates the count of frames for which transmission on a particular interface fails due to excessive collisions.

Graphing the Bridge tab using EDM

Use the following procedure to view read-only information about port frame statistics.

Procedure steps

1. In the **Device Physical View**, select one or multiple ports.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **Bridge** tab to view information about port frame statistics.

Variable definitions

The following table describes the fields of **Bridge** tab.

Field	Description
DelayExceededDiscards	Indicates the number of frames discarded by the port due to excessive transit delays through the bridge, incremented by both transparent and source route bridges.
MtuExceededDiscards	Indicates the number of frames discarded by the port due to an excessive size, incremented by both transparent and source route bridges.
InFrames	Indicates the number of frames that have been received by this port from its segment.
OutFrames	Indicates the number of frames that have been received by this port from its segment.
InDiscards	Indicates the count of valid frames received which were discarded (filtered) by the Forwarding Process.

Graphing the Rmon tab using EDM

Use the following procedure to view read-only remote monitoring statistics.

Procedure steps

1. In the **Device Physical View**, select one or multiple ports.
2. From the navigation tree, double-click **Graph**.

Comments? infodev@avaya.com

3. In the Graph tree, double-click **Port**.
4. In the work area, click the Rmon tab to view information about remote monitoring statistics.

Variable definitions

The following table describes the fields of Rmon tab.

Field	Description
Octets	Indicates 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	Indicates the total number of packets (including bad packets, broadcast packets, and multicast packets) received.
BroadcastPkts	Indicates the total number of good packets received that were directed to the broadcast address. This does not include multicast packets.
MulticastPkts	Indicates the total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
CRCAlignErrors	Indicates the total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
UndersizePkts	Indicates the total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
OversizePkts	Indicates the total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
Fragments	Indicates the total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Normal behavior is for etherStatsFragments is to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.

Field	Description
Collisions	Indicates the best estimate of the total number of collisions on this Ethernet segment.
Jabbers	Indicates the total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (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 a packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
1..64	Indicates the total number of packets (including bad packets) received that were between 1 and 64 octets in length (excluding framing bits but including FCS octets).
65..127	Indicates the total number of packets (including bad packets) received that were between 65 and 127 octets in length (excluding framing bits but including FCS octets).
128..255	Indicates the total number of packets (including bad packets) received that were between 128 and 255 octets in length (excluding framing bits but including FCS octets).
256..511	Indicates the total number of packets (including bad packets) received that were between 256 and 511 octets in length (excluding framing bits but including FCS octets).
511..1023	Indicates the total number of packets (including bad packets) received that were between 511 and 1023 octets in length (excluding framing bits but including FCS octets).
1024..1518	Indicates the total number of packets (including bad packets) received that were between 1024 and 1518 octets in length (excluding framing bits but including FCS octets).

Graphing the EAPOL Stats tab using EDM

Use the following procedure to view read-only EAPOL statistics.

Procedure steps

1. In the **Device Physical View**, select one or multiple ports.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **EAPOL Stats** tab to view information about EAPOL statistics.

Comments? infodev@avaya.com

Variable definitions

The following table describes the fields of **EAPOL Stats** tab.

Field	Description
EapolFramesRx	Indicates the number of valid EAPOL frames that have been received by this authenticator.
EapolFramesTx	Indicates the number of EAPOL frame types that have been transmitted by this authenticator.
EapolStartFramesRx	Indicates the number of EAPOL start frames that have been received by this authenticator.
EapolLogoffFramesRx	Indicates the number of EAPOL Logoff frames that have been received by this authenticator.
EapolRespIdFramesRx	Indicates the number of EAPOL Resp/Id frames that have been received by this authenticator.
EapolRespFramesRx	Indicates the number of valid EAP Response frames (other than Resp/Id frames) that have been received by this authenticator.
EapolReqIdFramesTx	Indicates the number of EAPOL Req/Id frames that have been transmitted by this authenticator.
EapolReqFramesTx	Indicates the number of EAP Req/Id frames (Other than Rq/Id frames) that have been transmitted by this authenticator.
InvalidEapolFramesRx	Indicates the number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EapLengthErrorFramesRx	Indicates the number of EAPOL frames that have been received by this authenticator in which the packet body length field is not valid.

Viewing and graphing the EAPOL Diag tab using EDM

Use the following procedure to view read-only EAPOL diagnostic statistics.

Procedure steps

1. In the **Device Physical View**, select one or multiple ports.
2. From the navigation tree, double-click **Graph**.

3. In the Graph tree, double-click **Port**.
4. In the work area, click the EAPOL Diag tab to view information about EAPOL diagnostic statistics.

Variable definitions

The following table describes the fields of **EAPOL Diag** tab.

Field	Description
EntersConnecting	Counts the number of times that the Authenticator PAE state machine transitions to the Connecting state from another state.
EapLogoffsWhileConnecting	Counts the number of times that the Authenticator PAE state machine transitions from Connected to Disconnected as a result of receiving an EAPOL-Logoff message.
EntersAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Connecting to Authenticating as a result of receiving an EAP-Response/Identity message from the supplicant.
AuthSuccessWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Authenticated as a result of the Backend authentication state machine indicating successful authentication of the supplicant.
AuthTimeoutsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of the Backend authentication state machine indicating authentication timeout.
AuthFailWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Held as a result of the Backend authentication state machine indicating authentication failure.
AuthReauthsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine

Comments? infodev@avaya.com

Field	Description
	transitions from Authenticating to Aborting as a result of a reauthentication request.
AuthEapStartsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPOL-Start message being received from the supplicant.
AuthEapLogoffWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPOL-Logoff message being received from the supplicant.
AuthReauthsWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of a reauthentication request.
AuthEapStartsWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of an EAPOL-Start message being received from the supplicant.
AuthEapLogoffWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Disconnected as a result of an EAPOL-Logoff message being received from the supplicant.
BackendResponses	Counts the number of times that the Backend Authentication state machine sends an Initial-Access request packet to the Authentication server.
BackendAccessChallenges	Counts the number of times that the Backend Authentication state machine receives an Initial-Access challenge packet from the Authentication server.
BackendOtherRequestsToSupplicant	Counts the number of times that the Backend Authentication state machine sends an EAP request packet (other than an Identity, Notification, failure, or success message) to the supplicant.

Field	Description
BackendNonNakResponsesFromSupplicant	Counts the number of times that the Backend Authentication state machine receives a response from the supplicant to an initial EAP request and the response is something other than EAP-NAK.
BackendAuthSuccesses	Counts the number of times that the Backend Authentication state machine receives an EAP-success message from the Authentication server.
BackendAuthFails	Counts the number of times that the Backend Authentication state machine receives an EAP-failure message from the Authentication server.

Graphing the LACP tab using EDM

Use the following procedure to view read-only Link Aggregation Control Protocol (LACP) diagnostic statistics.

Important:

The Marker Protocol Generator/Receiver is currently not a supported feature.

Procedure steps

1. In the **Device Physical View**, select one or multiple ports.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **LACP** tab to view information about LACP diagnostic statistics.

Variable definitions

The following table describes the fields of **LACP** tab.

Field	Description
LACPDUsRX	Denotes the number of valid LACPDUs received on this Aggregation Port. This value is read-only.

Comments? infodev@avaya.com

Field	Description
MarkerPDUsRX	Signifies the number of valid Marker PDUs received on this Aggregation Port. This value is read-only.
MarkerResponsePDUsRX	The number of valid Marker Response PDUs received on this Aggregation Port. This value is read-only.
UnknownRX	Indicates the number of frames received that can • Carry the Slow Protocols Ethernet Type value (43B.4), but contain an unknown PDU. • Are addressed to the Slow Protocols group MAC Address (43B.3), but do not carry the Slow Protocols Ethernet Type. This value is read-only.
IllegalRX	Denotes the number of frames received that carry the Slow Protocols Ethernet Type value (43B.4), but contain a badly formed PDU or an illegal value of Protocol Subtype (43B.4). This value is read-only.
LACPDUsTX	Signifies the number of LACPDUs that are transmitted on this Aggregation Port. This value is read-only.
MarkerPDUsTX	Displays the number of Marker PDUs transmitted on this Aggregation Port. This value is read-only.
MarkerResponsePDUsTX	Indicates the number of Marker Response PDUs that are transmitted on this Aggregation Port. This value is read-only.

Graphing the Misc tab

Use the following procedure to view statistical information that does not belong grouped with the other tabs.

Procedure steps

1. In the **Device Physical View**, select one or multiple ports.
2. From the navigation tree, double-click **Graph**.

3. In the Graph tree, double-click **Port**.
4. In the work area, click the **Misc** tab.

Variable definitions

The following table describes the fields of **Misc** tab.

Field	Description
NoResourcesPktsDropped	Indicates the number of packets dropped due to a lack of resources.

Graphing multilink trunk statistics using EDM

This section describes the procedures you can use to view Multilink Trunk (MLT) statistical information in a variety of graphs.

Accessing MLT statistics window

Use the following procedure to access the MLT statistics window.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the **Multilink Trunk** tab, select a row that represents the MLT.
4. On the toolbar, click **Graph** to view the MLT statistics.

Viewing the Interface tab using EDM

Use the following procedure to view read-only statistical information about the selected Multilink Trunk.

Comments? infodev@avaya.com

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the **Multilink Trunk** tab, select a row that represents the MLT.
4. On the toolbar, click **Graph** .

   The Multilink Trunks- Graph, 1 screen appears.
5. In the work area click the **Interface** tab.

Variable definitions

The following table describes the fields of **Interface** tab.

Field	Description
InMulticastPkts	Indicates the number of packets delivered to this MLT that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.
OutMulticastPkts	Indicates the total number of packets that higher-level protocols requested be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
InBroadcastPkts	Indicates the number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
OutBroadcastPkts	Indicates the total number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.
HCInOctets	Indicates the total number of octets received on the MLT interface, including framing characters.
HCOutOctets	Indicates the total number of octets transmitted out of the MLT interface, including framing characters.
HCInUcastPkts	Indicates the number of packets delivered by this MLT to higher level protocols that were not addressed to a multicast or broadcast address at this sublayer.
HCOutUcastPkts	Indicates the number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast

Field	Description
	address at this MLT. This total number includes those packets discarded or unsent.
HCInMulticastPkt	Indicates the number of packets delivered to this MLT that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.
HCOutMulticast	Indicates the total number of packets that higher-level protocols requested be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
HCInBroadcastPkt	Indicates the number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
HCOutBroadcast	Indicates the total number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.

Viewing the Ethernet Errors tab using EDM

Use the following procedure to view read-only statistical information about Ethernet errors that have occurred on the selected Multilink Trunk.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **MLT/LACP**.
3. In the **Multilink Trunk** tab, select a row that represents the MLT.
4. On the toolbar, click **Graph** .

   The Multilink Trunks- Graph, 1 screen appears.
5. In the work area click the **Ethernet Errors** tab.

Variable definitions

The following table describes the fields of **Ethernet Errors** tab.

Comments? infodev@avaya.com

Field	Description
AlignmentErrors	Indicates the count of frames received on a particular MLT that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented after 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	Indicates the count of frames received on an MLT 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 after the frameCheckError 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.
IMacTransmitError	Indicates the count of frames for which transmission on a particular MLT 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.
IMacReceiveError	Indicates the count of frames for which reception on a particular MLT 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 may represent a count of receive errors on a particular interface that are not otherwise counted.
CarrierSenseErrors	Indicates the number of times that the carrier sense condition was lost or never asserted after attempting to transmit a frame on a particular MLT. The count represented by an instance of this object is incriminated at most once for each transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
FrameTooLong	Indicates the count of frames received on a particular MLT that exceed the maximum permitted frame size.

Field	Description
	The count represented by an instance of this object is incremented after the frameTooLong 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.
SQETestError	Indicates the count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular MLT. 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.
DeferredTransmiss	Indicates the count of frames for which the first transmission attempt on a particular MLT is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollFrames	Indicates the count of successfully transmitted frames on a particular MLT 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.
MultipleCollFrames	Indicates the count of successfully transmitted frames on a particular MLT for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	Indicates the number of times that a collision is detected on a particular MLT 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.
ExcessiveColls	Indicates the count of frames for which transmission on a particular MLT fails due to excessive collisions.

Comments? infodev@avaya.com

Graphing VLAN DHCP statistics using EDM

Use the following procedure to create a graph of VLAN DHCP configuration.

Procedure steps

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, double-click **VLANs**.
3. In the work area, select the desired VLAN.
4. In the toolbar, click **IP**.

   The IP, VLAN 1 tab appears.
5. In the work area, click the **DHCP** tab.
6. In the toolbar, click **Graph**.

   The DHCP-Graph tab appears.
7. In the work area, highlight the required data.
8. In the toolbar, click the type of graph you want to produce.

Variable definitions

The following table explains the fields found on this window.

Field	Description
NumRequests	Indicates the number of DHCP requests handled.
NumReplies	Indicates the number of DHCP replies handled.

Viewing unit statistics using EDM

Use the following procedure to view the statistical information of a unit.

Procedure steps

1. In the **Device Physical View**, select the unit.
2. From the navigation tree, double-click **Edit**.
3. In the Edit tree, double-click **Unit**.
4. In the work area, click the **Unit Stats** tab to view the statistical information of the selected unit.

Variable definitions

The following table describes the fields of **Unit Stats** tab.

Field	Description
Absolute Value	Indicates the counter value of packets dropped for the unit.
Cumulative	Indicates the total value of packets dropped seen since dialog displayed.
Average/sec	Indicates the average value of packets dropped per second.
Minimum/sec	Indicates the smallest value of packets dropped seen per second.
Maximum/sec	Indicates the largest value of packets dropped seen per second.
LastVal/sec	Indicates the last value of packets dropped seen per second.

Comments? infodev@avaya.com

Chapter 10: RMON configuration using Enterprise Device Manager

This chapter describes the configuration and management of RMON using Enterprise Device Manager (EDM).

Working with RMON information using EDM

RMON information is viewed by looking at the graphing information associated with the port or chassis.

Viewing statistics using EDM

EDM gathers Ethernet statistics that can be graphed in a variety of formats or saved to a file that can be exported to an outside presentation or graphing application.

Use the following procedures to view RMON ethernet statistics.

Procedure steps

1. In the **Device Physical View**, select a port.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.

   OR

   Right-click the port, and choose **Graph**.

   The Graph Port screen appears.
4. In the work area, click the **Rmon** tab to view RMON ethernet statistics.

Variable definitions

The following table describes the fields on the Rmon tab.

Field	Descriptions
Octets	Indicates 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	Indicates the total number of packets (including bad packets, broadcast packets, and multicast packets) received.
BroadcastPkts	Indicates the total number of good packets received that were directed to the broadcast address. This does not include multicast packets.
MulticastPkts	Indicates the total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
CRCAlignErrors	Indicates the total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
UndersizePkts	Indicates the total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
OversizePkts (>1518)	Indicates the total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
Fragments	Indicates the total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Normal behavior for etherStatsFragments is to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Collisions	Indicates the best estimate of the total number of collisions on this Ethernet segment.
Jabbers	Indicates the total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (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 a packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.

Comments? infodev@avaya.com

Field	Descriptions
1..64	Indicates the total number of packets (including bad packets) that were transmitted and received on this port between 1 and 64 octets in length (excluding framing bits but including FCS octets).
65..127	Indicates the total number of packets (including bad packets) that were transmitted and received on this port between 65 and 127 octets in length (excluding framing bits but including FCS octets).
128..255	Indicates the total number of packets (including bad packets) that were transmitted and received on this port between 128 and 255 octets in length (excluding framing bits but including FCS octets).
256..511	Indicates the total number of packets (including bad packets) that were transmitted and received on this port between 256 and 511 octets in length (excluding framing bits but including FCS octets).
512..1023	Indicates the total number of packets (including bad packets) that were transmitted and received on this port between 512 and 1023 octets in length (excluding framing bits but including FCS octets).
1024..1518	Indicates the total number of packets (including bad packets) that were transmitted and received on this port between 1024 and 1518 octets in length (excluding framing bits but including FCS octets).

Statistic	Description
Poll Interval	Statistics are updated based on the poll interval. The default value is 10s. Valid range is None, 2s, 5s, 10s, 30s, 1m, 5m, 30m 1h.
Absolute	Indicates the total count since the last time counters were reset. A system reboot resets all counters.
Cumulative	Indicates the total count since the statistics tab was first opened. The elapsed time for the cumulative counter is shown at the bottom of the graph window.
Average/sec	Indicates the cumulative count divided by the cumulative elapsed time.
Minimum/sec	Indicates the minimum average for the counter for a polling interval over the cumulative elapsed time.
Maximum/sec	Indicates the maximum average for the counter for a polling interval over the cumulative elapsed time.
LastVal/sec	Indicates the average for the counter over the last polling interval.

Viewing 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:

- Buckets are gathered at 30-minute intervals.
- Number of buckets gathered is 50.

Both the time interval and the number of buckets is configurable. After the last bucket is reached, bucket 1 is dumped and "recycled" to hold a new bucket of statistics. Then bucket 2 is dumped.

Use the following procedure to view RMON history.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **RMON**.
3. In the RMON tree, double-click **Control**.
4. In the work area, click the **History** tab to view RMON history.

Variable definitions

The following table describes the fields of the **History** tab.

Field	Description
Index	Indicates a unique value assigned to each interface. An index identifies an entry in a table.
Port	Indicates an Ethernet interface on the device.
BucketsRequested	Indicates 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	Indicates the number of discrete sampling intervals over which data is saved in the part of the media-specific table associated with this entry. There are instances after the actual number of buckets associated with this entry is less than the value of this object. In this case, at the end of each sampling interval, a new bucket is added to the media-specific table.

Comments? infodev@avaya.com

Field	Description
Interval	Indicates 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 a number of seconds between 1 and 3600 (1 hour). Because the counters in a bucket may overflow at their maximum value with no indication, note the possibility of overflow in the associated counters. Consider the minimum time in which a counter could overflow on a particular media type and set the historyControlInterval object to a value less than this interval. This interval is typically most important for the octets counter in a media-specific table. For example, on an Ethernet network, the etherHistoryOctets counter could overflow in about one hour at the Ethernet's maximum utilization.
Owner	Indicates the network management system that created this entry.

Creating a history using EDM

RMON can be used to collect statistics at intervals. For example, if switch performance is monitored over a weekend, enough buckets to cover two days must be set aside. To do this, set the history to gather one bucket each hour, thus covering a 48-hour period. After history characteristics are set, they cannot be modified; the history must be deleted and another created.

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

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **RMON**.
3. In the RMON tree, double-click **Control**.
4. In the work area, click the **History** tab.
5. In the toolbar, click **Insert**.

   The Insert History dialog box appears.
6. In the fields provided, enter the information for the new RMON history.
7. Click **Insert**.

Variable Definitions

The following table describes the fields of the Insert History dialog box.

Field	Description
Index	Indicates a unique value assigned to each interface. An index identifies an entry in a table.

Field	Description
Port	Indicates any Ethernet interface on the device.
BucketsRequested	Indicates 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.
Interval	Indicates 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 a number of seconds between 1 and 3600 (1 hour). Because the counters in a bucket may overflow at their maximum value with no indication, note the possibility of overflow in the associated counters. Consider the minimum time in which a counter could overflow on a particular media type and set the historyControlInterval object to a value less than this interval. This interval is typically most important for the octets counter in a media-specific table. For example, on an Ethernet network, the etherHistoryOctets counter could overflow in about one hour at the Ethernet's maximum utilization.
Owner	Indicates the network management system that created this entry.

Disabling history using EDM

Use the following procedure to disable RMON history on a port.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **RMON**.
3. In the RMON tree, double-click **Control**.
4. In the **History** tab, select the row that contains the record you want to delete.
5. In the toolbar, click **Delete**.

Viewing RMON history statistics using EDM

Use the following procedure to display Rmon History statistics.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **RMON**.
3. In the RMON tree, double-click **Control**.

Comments? infodev@avaya.com

4. In the work area, select a port.
5. In the toolbar, click **Display History Data**.

   The Rmon History window appears for the selected port.

Variable definitions

The following table describes the fields of Rmon History screen.

Field	Description
SampleIndex	Indicates the sample number. As history samples are taken, they are assigned greater sample numbers.
Utilization	Estimates the percentage of a link's capacity that was used during the sampling interval.
Octets	Indicates the number of octets received on the link during the sampling period.
Pkts	Indicates the number of packets received on the link during the sampling period.
BroadcastPkts	Indicates the number of packets received on the link during the sampling interval that were destined for the broadcast address.
MulticastPkts	Indicates the number of packets received on the link during the sampling interval that are destined for the multicast address. This does not include the broadcast packets.
DropEvents	Indicates the number of received packets that were dropped because of system resource constraints.
CRCAlignErrors	Indicates the number of packets received during a sampling interval that were between 64 and 1518 octets long. This length included Frame Check Sequence (FCS) octets but not framing bits. The packets had a bad FCS with either an integral number of octets (FCS Error), or a non-integral number of octets (Alignment Error).
UndersizePkts	Indicates the number of packets received during the sampling interval were less than 64 octets long (including FCS octets, but not framing bits.
OversizePkts	Indicates the number of packets received during the sampling interval were longer than 1518 octets (including FCS octets, but not framing bits, and were otherwise well formed.
Fragments	Indicates 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 octects (FCS Error), or a non-integral number of octets (Alignment Error).
Collisions	Indicates the best estimate of the number of collisions on an Ethernet segment during a sampling interval.

Enabling ethernet statistics gathering using EDM

Use the following procedure to gather ethernet statistics.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **RMON**.
3. In the RMON tree, double-click **Control**.
4. In the work area, click the **Ether Stats** tab.
5. In the toolbar, click **Insert**.

   The Insert Ether Stats dialog box appears.
6. Enter the port number you want to use in the **Port** field. You can either type the port number, or click Port ellipse (**...**) to select a port number from the Port List..
7. Type the owner of this RMON entry in the **Owner** field.
8. Click **Insert**.

Variable definitions

The following table describes the fields of Insert Ether Stats screen.

Field	Description
Index	Indicates a unique value assigned to each interface. An index identifies an entry in a table.
Port	Indicates a port on the device.
Owner	Indicates the network management system that created this entry.

Disabling Ethernet statistics gathering using EDM

Use the following procedure to disable Ethernet statistics.

Prerequisites

- Open one of the supported browsers.
- Enter the IP address of the switch to open an EDM session.

Comments? infodev@avaya.com

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **RMON**.
3. In the RMON tree, double-click **Control**.
4. In the work area, click the **Ether Stats** tab.
5. Select the row that contains the record that you want to delete.
6. In the toolbar, click **Delete**.

Configuring Alarm Manager using EDM

This section describes the procedure you can use for Alarm Manager.

Creating an Alarm using EDM

Use the following procedure to create an alarm to receive statistics and history using default values.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **RMON**.
3. In the RMON tree, double-click **Alarms**.
4. In the work area, click the **Alarms** tab.
5. In the toolbar, click **Insert**.

   The Insert Alarm dialog box appears.
6. Configure the parameters as required for the alarm.
7. Click **Insert**.

Variable definitions

The following table describes the fields of Insert Alarm dialog box.

Field	Description
Variable	Indicates the name and type of alarm.

Field	Description
	alarmname.x Here x=0 indicates a chassis alarm. *alarmname.* where the user must specify the index. This index is a card number for module-related alarms, an STG ID for spanning tree group alarms (the default STG is 1, other STG IDs are user-configured), or the Ether Statistics Control Index for RMON Stats alarms *alarmname* with no dot or index is a port-related alarm and results in display of the port selection tool.
Sample Type	Indicates the sample type. Available options are: • absoluteValue • deltaValue
Interval	Indicates 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 such entry defines a diagnostic sample at a particular interval for an object on the device.
RisingThreshold	Generates a single events if 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.
RisingEventIndex	Indicates 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 filled in.)
RisingThreshold	Generates a single event if the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold.
FallingEventIndex	Indicates 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 filled in.)
Owner	Indicates the network management system that created this entry.

Deleting an alarm using EDM

Use the following procedure to delete an alarm.

Comments? infodev@avaya.com

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **RMON**.
3. In the RMON tree, double-click **Alarms**.
4. In the work area, click the **Alarms** tab.
5. Select the alarm you want to delete.
6. In the toolbar, click **Delete**.

Variable definitions

The following table describes the fields on the **Alarms** tab.

Field	Description
Index	Uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device.
Interval	Indicates the interval in seconds over which data is sampled and compared with the rising and falling thresholds. After setting this variable, in the case of deltaValue sampling, you should set the interval short enough that the sampled variable is very unlikely to increase or decrease by a delta of more than 2^31 - 1 during a single sampling interval.
Variable	Indicates the object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Counter, Gauge, or TimeTicks) may be sampled.
Sample Type	Indicates the method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue(2), the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.
Value	Indicates the value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value is the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value is the sampled value at the end of the period. This value is compared with the rising and falling thresholds. The value during the current sampling period is not made available until the period is completed and remains available until the next period is completed.

Field	Description
StartupAlarm	Indicates the alarm that may be sent after this entry is first set to Valid. If the first sample after this entry becomes valid is greater than or equal to the risingThreshold and alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3), a single rising alarm is generated. If the first sample after this entry becomes valid is less than or equal to the fallingThreshold and alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3) a single falling alarm is generated.
RisingThreshold	Indicates the threshold for the sampled statistic. After 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, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3). After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold.
RisingEventIndex	Indicates the index of the eventEntry that is used after a rising threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable no association exists. In particular, if this value is zero, no associated event is generated, because zero is not a valid event index.
FallingThreshold	Indicates the threshold for the sampled statistic. After the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold and the associated alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3). After a falling event is generated, another such event is not generated until the sampled value rises above this threshold and reaches the alarmRisingThreshold.
FallingEventIndex	Indicates the index of the eventEntry that is used after a falling threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable no association exists. In particular, if this value is zero, no associated event is generated, because zero is not a valid event index.
Owner	Indicates the network management system that created this entry.
Status	Indicates the status of this alarm entry.

Comments? infodev@avaya.com

Configuring Events using EDM

This section describes how RMON events and alarms work together to provide notification after values in the network are outside of a specified range. After values pass the specified ranges, the alarm is triggered. The event specifies how the activity is recorded.

How events work

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

- RisingEvent
- FallingEvent

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 fires 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.

Viewing an event using EDM

Use the following procedure to view a table of events.

Procedure steps

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

Variable definitions

The following table describes the fields of **Events** tab.

Field	Description
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	Indicates the type of notification that the EDM 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: • none • log • trap • log-and-trap
Community	Indicates the SNMP community string acts as a password. Only those management applications with this community string can view the alarms.
LastTimeSent	Indicates the value of sysUpTime at the time this event entry last generated an event. If this entry has not generated events, this value is zero.
Owner	If traps are specified to be sent to the owner, this is the name of the machine which receives traps.

Creating an event using EDM

Use the following procedure to create an event.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **RMON**.
3. In the RMON tree, double-click **Alarms**.
4. In the work area, click the **Events** tab.
5. In the toolbar, click **Insert**.

   The Insert Events dialog box appears.
6. Configure the parameters as required.
7. Click **Insert**.

Comments? infodev@avaya.com

Variable definitions

The following table describes the fields of Insert Events screen.

Field	Description
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	Indicates the type of notification that EDM 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: • none • log • trap • log-and-trap
Community	Indicates the SNMP community string acts as a password. Only those management applications with this community string can view the alarms.
Owner	If traps are specified to be sent to the owner, this is the name of the machine receives alarm traps.

Deleting an event using EDM

Use the following procedure to delete an event.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **RMON**.
3. In the RMON tree, double-click **Alarms**.
4. In the work area, click the **Events** tab.
5. Select the event you want to delete from the list.
6. In the toolbar, click **Delete**.

Viewing log information using EDM

Use the following procedure to view the alarm activity.

Procedure steps

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

Variable definitions

The following table describes the fields of Log tab.

Item	Description
Time	Specifies the time an event occurred that activated the log entry.
Description	Specifies whether the event is a rising or falling event.
EventIndex	Specifies the index of the event.

Comments? infodev@avaya.com

Chapter 11: IPFIX configuration using Enterprise Device Manager

This section describes the configuration and management of IPFIX functionality using the Enterprise Device Manager (EDM).

Configuring Global IPFIX

IPFIX functionality can be globally enabled or disabled from the EDM. By default, IPFIX is disabled and you must enable it before it starts to collect flow information. This section contains the procedures for enabling and disabling IPFIX on a switch.

Use the following command to enable or disable IPFIX.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, click **IPFIX**.
3. In the **Global** tab work area, select the operational state of IPFIX functionality in the **State** area.
4. In the toolbar, click **Apply**.

Configuring IPFIX flows

After you enable IPFIX on a switch, you must configure the ports IPFIX monitors. Use the following procedure to configure IPFIX flows.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, click **IPFIX**.

3. In the work area, click the **Exporters** tab.

   The Exporters tab lists the IPFIX exporters that are currently available. If connected to a stand-alone unit, the export properties of that unit are listed. If connected to a stack, the export properties of all units in the stack are listed.
4. In the table, in the port row, double-click the cell under the column heading for the parameter you want to change.
5. Select a parameter or value from the drop-down list.
6. Repeat the previous two steps until you have amended all of the parameters you want to change.
7. In the toolbar, click **Apply**.

Variable definitions

The following table describes the fields of the **Exporters** tab.

Field	Description
Slot	Indicates the switch that is exporting IPFIX flows. This number corresponds to the unit number in a stack or is 1 for a stand-alone unit.
AgingIntv	Indicates the aging interval of the flow record in seconds. This value is an integer between 0 and 2147400.
ActiveTimeout	Indicates the flow record active timeout value in minutes.
ExportIntv	Indicates the frequency of data exports to the collector in seconds. This value is an integer between 10 and 3600.
ExportState	Indicates the current state of the exporter.
TempRefIntvSec	Indicates the template refresh time out in seconds. The template is sent out to the collector either at the interval specified in this value or after the number of packets specified in the **TempRefIntvPkts** value, whichever occurs first. This value is an integer between 300 and 3600.
TempRefIntvPkts	Indicates the template refresh time out in numbers of packets. The template is sent out to the collector either at the interval specified in this value or after the number of seconds specified in the **TempRefIntvSec** value, whichever occurs first. This value is an integer between 10000 and 100000.

Comments? infodev@avaya.com

Configuring IPFIX collectors

IPFIX collectors are used to collect and analyze data exported from an IPFIX-compliant switch. Up to two collectors can be supported.

The switch exports IPFIX data in *Netflow version 9* format using UDP port 9995.

IPFIX data is not load balanced when two collectors are in use. Identical information is sent to both collectors.

Use the following procedures to configure an IPFIX collector.

Creating a collector using EDM

Use the following procedure to create an IPFIX collector.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, click **IPFIX**.
3. In the work area, click the **Collectors** tab.
4. In the toolbar, click **Insert**.
5. In the work area, configure the parameters as required.
6. Click **Insert**.

Variable definitions

The following table describes the fields of the Insert Collectors dialog.

Field	Description
Slot	Indicates the unit number of the collector. Currently up to two collectors are supported so the values 1 or 2 are valid.
AddressType	Indicates the address type of the IP address of the collector. Currently only IPv4 addresses are supported.
Address	Indicates the IP address of the collector.
Protocol	Indicates the protocol used to transport the IPFIX data to the collector. Currently only the UDP protocol is supported for this task.

Field	Description
DestPort	Indicates the port on which the collector is listening for IPFIX data. Currently only port 9995 is supported for this task.
ProtoVer	Indicates the format in which IPFIX data is provided to the collector. Currently only Netflow version 9 formatting is supported for this task.
Enable	Indicates the operational state of this collector.

Modifying collectors

Use the following procedure to modify an IPFIX collector.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, click **IPFIX**.
3. In the work area, click the **Collectors** tab.
4. In the table, double-click a cell under the column heading for the parameter you want to change.
5. Select a parameter or value from the drop-down list.
6. Repeat the previous two steps until you have amended all of the parameters you want to change.
7. In the toolbar, click **Apply**.

Variable definitions

The following table describes the fields of **Collectors** tab.

Field	Description
Slot	Indicates the unit number of the collector. Currently up to two collectors are supported.
AddressType	Indicates the address type of the IP address of the collector. Currently only IPv4 addresses are supported.
Address	Indicates the IP address of the collector.
Protocol	Indicates the protocol used to transport the IPFIX data to the collector. Currently only the UDP protocol is supported for this task.

Comments? infodev@avaya.com

Field	Description
DestPort	Indicates the port on which the collector is listening for IPFIX data. Currently only port 9995 is supported for this task.
ProtoVer	Indicates the format in which IPFIX data is provided to the collector. Currently only Netflow version 9 formatting is supported for this task.
Enable	Indicates the operational state of this collector.

Deleting a collector

Use the following procedure to delete an IPFIX collector.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, click **IPFIX**.
3. In the work area, click the **Collectors** tab.
4. In the table, select the IPFIX collector you want to delete.
5. In the toolbar, click **Delete**.

Configuring IPFIX ports

Use the following procedure to configure IPFIX ports.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, click **IPFIX**.
3. In the work area, click **Ports** tab.
4. Click the Switch/Stack/Port ellipses (**...**) to select a port or multiple ports.
5. In the table, double-click a cell under the **Flush** column heading.
6. Choose a value or parameter from the drop-down list.

7. Repeat the previous two steps for the column heading **AllTraffic**.
8. Click **Apply Selection** to commit the changes.

   OR

   Click **Undo Apply** or **Clear Selection** to cancel the changes.

Variable definitions

The following table describes the fields of the **Ports** tab.

Field	Description
Id	Indicates the individual port on which the IPFIX parameters are being configured. Ports are itemized in the format *Unit / Port*.
Flush	Determines the flushing action to take on the port. Flushing the port of data involves deleting all previously gathered infotmation about that port. This field provides three options: • none - The port data is not flushed. • flush - The port data is flushed; deleting it from switch memory. • exportAndFlush - The port data is exported to a configured collector and the data is then flushed. Although this field is displayed on a per port basis, flushing is only supported on a per unit basis in Software Release 5.0.
AllTraffic	Determines whether IPFIX data is collected on this port. This field provides two options: • enable - IPFIX data is collected. • disable - IPFIX data is not collected.

Displaying IPFIX data information

Use this procedure to set the display criteria and display IPFIX data information.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, click **IPFIX**.
3. In the work area, click the **Data Information** tab.

Comments? infodev@avaya.com

Variable definitions

Variable	Value
Unit Number	Specifies whether the switch is a standalone or part of a stack. A value of 1 indicates a standalone switch. A value greater than 1 indicates the switch location in a stack.
Sort By	Specifies a rule to sort the data. Values include: • Source Address — source IP address • Destination Address — destination IP address • Protocol — protocol number • TOS — type of service • Port — port number • TCP/UDP Src Port — TCP/UDP source port • TCP/UDP Dst Port — TCP/UDP desitnation port • Packet Count — packet number • Byte Count — data byte number • First Packet Time — first packet time • Last Packet Time — last packet time
Sort Order	Specifies ascending or descending.
Display	Specifies the number of entries to display. Values include: • Top 10 • Top 25 • Top 50 • Top 100 • Top 200

Graphing Exporter Statistics using EDM

Use the following procedure to view IPFIX exporter statistics.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, click **IPFIX**.
3. In the work area, click the **Collectors** tab.
4. Select the record that you want to graph.
5. In the toolbar, click **Graph**.

Variable definitions

The following table outlines the fields on this tab.

Field	Description
OutPkts	Indicates the total number of packets sent.
OutOctets	Indicates the total number of bytes sent.
PktsLoss	Indicates the total number of records lost.

Viewing the IPFIX collector clear time

Use this procedure to display the system time after IPFIX exporter statistics were last cleared.

Procedure steps

1. From the navigation pane, double-click **Serviceability**.
2. In the Serviceabilitytree, click **IPFIX**.
3. In the IPFIX work area, click the **Collectors** tab.
4. Select the .record that you want to graph.

Comments? infodev@avaya.com

5. Click **Graph**.
6. Click the**Clear Time** tab.

Comments? infodev@avaya.com

Chapter 12: Topology configuration using Enterprise Device Manager

This section describes topology diagnostic information available in Enterprise Device Manager through the following tabs:

Viewing topology information

To view topology information:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **Topology**.
4. Select the **Topology** tab.

The following table outlines the parameters of the **Topology** tab.

Table 10: Variable definitions

Variable	Value
IpAddr	The IP address of the device.
Status	Whether Avaya topology is on (topOn) or off (topOff) for the device. The default value is topOn.
NmmLstChg	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, then the value is zero.
NmmMaxNum	The maximum number of entries in the NMM topology table.
NmmCurNum	The current number of entries in the NMM topology table.

Viewing topology table information

To view more topology information:

Procedure steps

1. From the navigation tree, double-click **Edit**.
2. From the Edit tree, double-click **Diagnostics**.
3. From the Diagnostics tree, double-click **Topology**.
4. Select the **Topology Table** tab.

The following table outlines the parameters of the **Topology Table** tab.

Table 11: Variable definitions

Variable	Value
Slot	The slot number in the chassis in which the topology message was received.
Port	The port on which the topology message was received.
IpAddr	The IP address of the sender of the topology message.
SegId (Slot/Port)	The segment identifier, slot , and port number from where the autotopology packets were received.
MacAddr	The MAC address of the sender of the topology message.
ChassisType	The chassis type of the device that sent the topology message.
BkplType	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	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.

Comments? infodev@avaya.com

Chapter 13: Configuring the SLA Monitor using ACLI

Use the procedures in this section to configure the SLA Monitor agent.

Displaying SLA Monitor agent settings

Use this procedure to view the global SLA Monitor agent settings.

Procedure

1. Enter Privileged EXEC mode:
   ```
   enable
   ```
2. At the command prompt, enter the following command:
   ```
   show application slamon agent
   ```

Example

```
5650TD>enable
5650TD#show application slamon agent
SLAMon Operational Mode: Enabled
SLAMon Agent Encryption: Not Supported
SLAMon Agent Address: 172.16.120.10
SLAMon Agent Port: 50011
SLAMon Agent Registration Status: Not Registered
SLAMon Registered Server Address: 0.0.0.0
SLAMon Registered Server Port: 0
SLAMon Server Registration Time: 0
SLAMon CLI Mode: Enabled
SLAMon CLI Timeout Mode: Enabled
SLAMon CLI Timeout: 60 seconds
SLAMon Configured Agent Address: 0.0.0.0
SLAMon Configured Agent Port: 0
SLAMon Configured Server Address: 0.0.0.0 0.0.0.0
SLAMon Configured Server Port: 0
SLAMon Agent-To-Agent Communication Port: 50012
SLAMon Configured Agent-To-Agent Communication Port: 0
SLAMon Agent Server Bypass: Disabled
SLAMon Agent Refuse Server Tests: Allow Tests
```

Configuring SLA Monitor using ACLI

Use this procedure to configure the SLA Monitor agent to communicate with an SLA Monitor server to perform Quality of Service (QoS) tests of the network.

Before you begin

To take full advantage of the SLA Monitor agent, you must have an SLA Monitor server in your network. The Quality of Service (QoS) tests can be performed without a server.

About this task

To configure the agent, you must enable the agent and assign an IP address. By default, the agent uses the switch/stack IP address if a specific agent address is not configured. Remaining agent parameters are optional and you can operate the agent using the default values.

Procedure

1. Enter Application Configuration mode:
   ```
   enable
   configure terminal
   application
   ```
2. To configure the agent IP address, enter the following command:
   ```
   slamon agent ip address {A.B.C.D}
   ```
3. To configure the agent IP address to its default value, enter the following command:
   ```
   default slamon agent ip address
   ```
4. To configure the UDP port, enter the following command:
   ```
   slamon agent port <0, 1024-65535>
   ```
5. To configure the agent UDP port to its default value, enter the following command:
   ```
   default slamon agent port
   ```
6. To enable the agent, enter the following command:
   ```
   slamon oper-mode enable
   ```
7. To disable the agent, enter the following command:
   ```
   no slamon oper-mode [enable]
   ```
   OR
   ```
   default slamon oper-mode
   ```
8. To configure the agent-to-agent communication port, enter the following command:
   ```
   slamon agent—comm—port <0, 1024-65535>
   ```


Comments? infodev@avaya.com

9. To configure the agent-to-agent communication port to its default value, enter the following command:

   ```
   default slamon agent—comm—port
   ```

10. To enable the SLA Monitor agent CLI support, enter the following command:

    ```
    slamon cli enable
    ```

    Note:

    This CLI command affects only the SLA Monitor CLI and not the standard platform CLI.

11. To disable the SLA Monitor agent CLI support, enter the following command:

    ```
    no slamon cli [enable]
    ```

    OR

    ```
    default slamon cli
    ```

    Note:

    These CLI commands affect only the SLA Monitor CLI and not the standard platform CLI.

12. To configure the agent automatic CLI session timeout value, enter the following command:

    ```
    [default] slamon cli-timeout <60-600>
    ```

    Note:

    This CLI command affects only the SLA Monitor CLI and not the standard platform CLI.

13. To enable the agent automatic CLI session timeout, enter the following command:

    ```
    slamon cli-timeout—mode enable
    ```

    OR

    ```
    default slamon cli-timeout—mode
    ```

    Note:

    These CLI commands affect only the SLA Monitor CLI and not the standard platform CLI.

14. To disable the agent automatic CLI session timeout, enter the following command:

    ```
    no slamon cli-timeout—mode [enable]
    ```

    Note:

    This CLI command affects only the SLA Monitor CLI and not the standard platform CLI.

15. To configure the agent server IP address, enter the following command:

```
slamon server ip address {A.B.C.D} [{A.B.C.D}]
```

16. To configure the agent server IP address to its default value, enter the following command:

    ```
    default slamon server ip address
    ```

17. To configure the server TCP registration port, enter the following command:

    ```
    slamon server port <0-65535>
    ```

18. To configure the server TCP registration port to its default value, enter the following command:

    ```
    default slamon server port
    ```

19. To enable the agent refuse server test mode, enter the following command:

    ```
    slamon refuse-server-tests [refuse]
    ```

20. To disable the agent refuse server test mode (i.e. allow the agent to accept test requests from the server), enter the following command:

    ```
    no slamon refuse-server-tests [refuse]
    ```

    OR

    ```
    default slamon refuse-server-tests
    ```

21. To enable the agent server bypass mode, enter the following command:

    ```
    slamon server-bypass [enable]
    ```

22. To disable the agent server bypass mode, enter the following command:

    ```
    no slamon server-bypass [enable]
    ```

    OR

    ```
    default slamon server-bypass
    ```

23. To display the SLA monitor configuration, enter the following command:

    ```
    show application slamon agent
    ```

Example

```
5650TD>enable
5650TD#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
5650TD(config)#application
5650TD(config-app)#slamon oper-mode enable
5650TD(config-app)#show application slamon agent
SLAMon Operational Mode: Enabled
SLAMon Agent Encryption: Not Supported
SLAMon Agent Address: 172.16.120.10
SLAMon Agent Port: 50011
SLAMon Agent Registration Status: Not Registered
SLAMon Registered Server Address: 0.0.0.0
SLAMon Registered Server Port: 0
SLAMon Server Registration Time: 0
SLAMon CLI Mode: Enabled
SLAMon CLI Timeout Mode: Enabled
```


Comments? infodev@avaya.com

```
SLAMon CLI Timeout: 60 seconds
SLAMon Configured Agent Address: 0.0.0.0
SLAMon Configured Agent Port: 0
SLAMon Configured Server Address: 0.0.0.0 0.0.0.0
SLAMon Configured Server Port: 0
SLAMon Agent-To-Agent Communication Port: 50012
SLAMon Configured Agent-To-Agent Communication Port: 0
SLAMon Agent Server Bypass: Disabled
SLAMon Agent Refuse Agent Server Tests: Allow Tests
5650TD(config-app)#
```

Next steps

If you have configured SLA Monitor but the agent is not functioning as expected, determine task status using the engineering menu.

If the agent is not in the expected state, reset the system to start the agent.

If the agent task functions as expected, perform typical troubleshooting steps to verify agent accessibility:

- Verify IP address assignment and port use.
- Verify that the SLA Monitor agent is enabled.
- Ping the server IP address.
- Verify the server configuration.

Variable definitions

The following table describes the parameters for the **slamon** command.

Variable	Value
agent-comm-port *<0, 1024–65535>*	Configures the SLA Monitor agent-to-agent communication UDP port. The default port is 50012. If you configure this value to zero (0), the default port is used.
agent ip address *<A.B.C.D>*	Configures the agent IP address. If no IP address is specified, the default value is 0.0.0.0, which causes the agent to use the switch/stack IP address.
agent port *<0, 1024–65535>*	Configures the UDP port for agent-server communication. The agent receives discovery packets on this port. The default is port 50011. The server must use the same port.
cli-timeout *<60–600>*	Configures the CLI timeout value in seconds. The default is 60 seconds.

Variable	Value
	Note: The CLI commands only impact the SLA Monitor CLI and not the standard platform CLI.
oper-mode enable	Enables the SLA Monitor agent. The default is disabled. If you disable the agent, it does not respond to discover packets from a server. If you disable the agent because of resource concerns, consider changing the server configuration instead, to alter the test frequency or duration, or the number of targets.
server ip address *{A.B.C.D} [{A.B.C.D}]*	Restricts the agent to use of this server IP address only. The default is 0.0.0.0, which means the agent can register with any server. You can specify a secondary server as well.
server port <*0–65535*>	Restricts the agent to use of this registration port only. The default is 0, which means the agent disregards the source port information in server traffic. The server must use the same port.
refuse-server-tests [refuse]	Agent rejects NTR and RTP test requests from the server. If you disable this mode, the agent accepts test requests from the server with which it is registered. Test requests originating from platform, SLM CLI interfaces, and SNMP are not affected.
server-bypass enable	Allows an enabled agent to always accept agent-to-agent traffic. When enabled a small number of network ports remain open to process network traffic. You must take this into account if security concerns are high.

Comments? infodev@avaya.com

Executing a new trace route test

Use this procedure to execute a new trace route (NTR) test on the network to establish the Quality of Service (QoS) benchmark.

Before you begin

To execute the NTR test, you must enable the agent and assign an IP address.

Procedure

1. Enter Application Configuration mode:

   ```
   enable
   configure terminal
   application
   ```

2. At the command prompt, enter the following command:

   ```
   slamon ntr <A.B.C.D> <0-63> [[attempts <1-10>] | [period <1000-200000>]]
   ```

Example

```
5650TD>enable
5650TD#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
5650TD(config)#application
5650TD(config-app)#slamon oper-mode enable
5650TD(config-app)#slamon ntr 10.30.56.100 46

-----------------------------------------------------
SLAMon Network Trace Report
-----------------------------------------------------
Source IP/Port: 10.30.56.193:50013
Source DSCP Marking: 46
Destination IP/Port: 10.30.56.100:33434
Maximum TTL: 1
Request Result: OK (Port unreachable)
                  Ingress  Egress
IP Address         DSCP     DSCP      RTT (ms)
-----------------------------------------------------
10.30.56.193        46        0       0.000
10.30.56.100         0        0       1.240
5650TD(config-app)#
```

Variable definitions

The following table describes the parameters for the **slamon ntr** command.

Variable	Value
<A.B.C.D>	Specifies the destination IP address. If no IP address is specified, the test execution fails.
<0–63>	Specifies the Differential Services Code Point (DSCP) value for use in packets that are generated by the NTR test
attempts *<1–10>*	Specifies the number of attempts generated by the NTR test. DEFAULT: 2
period *<1000–200000>*	Specifies the interval between packets in microseconds, generated by the NTR test. The default interval is 20000 microseconds. DEFAULT: 20000

Executing a real time protocol test

Use this procedure to execute a real time protocol (RTP) test on the network to establish the Quality of Service (QoS) benchmark.

Before you begin

To execute the RTP test, you must enable the agent and assign an IP address.

Note:

If the RTP target is not registered with a server, you must enable the SLA Monitor agent ServerBypass mode for the RTP test to complete successfully.

Procedure

1. Enter Application Configuration mode:

   ```
   enable
   configure terminal
   application
   ```

2. To execute the RTP test, enter the following command::

Comments? infodev@avaya.com

```
slamon rtp <A.B.C.D> <0-63> [ [npack <10-100>] | [nsync <10-
100>] | period <1000-200000>]]
```

Example

```
5650TD>enable
5650TD#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
5650TD(config)#application
5650TD(config-app)#slamon oper-mode enable
5650TD(config-app)#slamon rtp 10.30.56.100 46

-----------------------------------------------------
SLAMon Real Time Protocol Network Report
-----------------------------------------------------
Source IP/Port: 10.30.56.193:50012
Source DSCP Marking: 46
Destination IP/Port: 10.30.56.100:50012

Delay (RTT): average 1.824 (ms)  median 1.701 (ms)
Packet Loss: 0

Out-of-Order Arrivals:0

-------------------------------------------------
          Network Jitter - Quartiles (ms)
    0         1         2         3         4
-------------------------------------------------
    0.007     0.173     0.208     0.224     1.343
5650TD(config-app)#
```

Variable definitions

The following table describes the parameters for the **`slamon rtp`** command.

Variable	Value
<A.B.C.D>	Specifies the destination IP address. If no IP address is specified, the test execution fails.
<0–63>	Specifies the differential services code point (DSCP) value for use in packets that are generated by the RTP test.
npack *<10–100>*	Specifies the RTP npack value. DEFAULT: 50
nsync *<10–100>*	Specifies the RTP nsync value. DEFAULT: 10

Variable	Value
period <*1000–200000*>	Specifies the interval between packets in microseconds, generated by the RTP test. DEFAULT: 20000

Comments? infodev@avaya.com

Chapter 14: Configuring the SLA Monitor using EDM

Use the procedures in these sections to configure the settings for SLA Monitor using EDM.

Configuring SLA Monitor

Use this procedure to configure SLA Monitor.

Procedure

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, click **SLA Monitor**.
3. In the SLA Monitor tab, configure the parameters as required..
4. On the toolbar, click **Apply**.

SLA Monitor tab field descriptions

Name	Description
Status	Enables or disables the SLA Monitor agent. The default is disabled. • **enabled**: enables the SLA Monitor agent • **disabled**: disables the SLA Monitor agent If you disable the agent, it does not respond to discover packets from a server. If you disable the agent because of resource concerns, consider changing the server configuration instead, to alter the test frequency or duration, or the number of targets.

Name	Description
ServerBypass	Enables or disables the server bypass mode. The default is disable. • **enable**: enables an agent to respond to agent-to-agent test requests regardless of the server registration status. • **disable**: restricts agent responses when the agent is not registered with an SLA Monitor server.
RefuseServerTests	Sets the attribute to determine whether the SLA Monitor agent will refuse test requests from the server. • **allow**: enables an agent to accept test requests from the server. • **refuse**: causes the agent to reject test requests from the server.
ConfiguredAgentToAgentPort	Specifies the UDP port utilized by the SLA Monitor agent for agent-agent communication. If the value is 0, the SLA Monitor agent will utilize a default port value for the base agent-agent UDP communication port.
ConfiguredAgentAddrType	Indicates IPv4–based communications.
ConfiguredAgentAddr	Specifies the agent IP address. The default value is 0.0.0.0, which cases the agent to use the switch/stack IP address.
ConfiguredAgentPort	Specifies the UDP port for agent-server communication. The agent receives discovery packets on this port. The default is port 50011. The server must use the same port.
CliAvailable	Specifies whether SLA Monitor agent CLI is available or not available. **Note:** This affects only the SLA Monitor CLI and not the standard platform CLI.
CliTimeout	Configures the CLI timeout value in seconds. The default is 60 seconds. **Note:** This affects only the SLA Monitor CLI and not the standard platform CLI.

Comments? infodev@avaya.com

Name	Description
CliTimeoutMode	Configures whether the agent automatic CLI session timeout is enabled or disabled. **Note:** This affects only the SLA Monitor CLI and not the standard platform CLI.
ConfiguredServerAddrType	Indicates IPv4–based communications.
ConfiguredServerAddr	Specifies the server IP address. If an IP address is specified, the agent is restricted to use this server IP address. The default is 0.0.0.0, which allows the agent to register with any server.
ConfiguredServerPort	Specifies the server port. The default is 0, which allows the agent to disregard the source port information in server traffic. The server must use the same port.
ConfiguredAltServerAddrType	Indicates IPv4–based communications.
ConfiguredAltServerAddr	Specifies a secondary server IP address.
SupportApps	Indicates SLA Monitor supported applications. This is a read-only field.
AgentAddressType	Indicates IPv4–based communications. This is a read-only field.
AgentAddress	Indicates the agent IP address. This is a read-only field.
AgentPort	Indicates the agent port. This is a read-only field.
RegisteredWithServer	Indicates whether the agent is registered with a server. This is a read-only field.
RegisteredServerAddrType	Indicates IPv4–based communications. This is a read-only field.
RegisteredServerAddr	Indicates the IP address of the SLA Monitor server with which the agent is registered .This is a read-only field.
RegisteredServerPort	Indicates the server TCP registration port . This is a read-only field.
RegistrationTime	Indicates the time in seconds since the agent registered with the server. This is a read-only field.
AgentToAgentPort	Indicates the base UDP port currently used by the SLA Monitor agent for agent-agent

Name	Description
	communication. The base UDP port is used to derive multiple agent communication ports. This is a read-only field.
EncryptionSupport	Indicates whether encrypted agent-server communication is supported by the agent. Secure images utilize encryption while non-secure images do not. This is a read-only field.

Executing NTR test

Use this procedure to execute an NTR test on the network to establish QoS benchmark.

Before you begin

You must enable the SLA Monitor CLI support to execute NTR tests in the absence of an SLA Monitor server.

About this task

Important:

When executing the script using EDM, do not run other commands while the script is in progress, because this slows down the execution. EDM can time-out while waiting for a response and even when a time-out occurs, the script execution continues on EDM.

Procedure

1. From the navigation tree, double-click **Serviceability**.
2. In the **Serviceability** tree, double-click **SLA Monitor**.
3. In the **SLA Monitor** work area, click the **NTR** tab.
4. Click **Insert**.
5. In the **OwnerId** field, type an owner id.
6. In the **TestName** field, type the test name.
7. In the **TargetAddress** field, type an IP address.
8. In the **Dscp** field, type a dscp value.
9. In the **Attempts** field, enter a value.
10. In the **Period** field, enter a value.
11. In the **AdminStatus** section, select **enabled**.
12. In the **Label** section, enter a character string.

Comments? infodev@avaya.com

13. Click **Insert** to initiate the NTR test.

Next steps

To view the test results, click **Results**.

NTR tab field descriptions

Name	Description
OwnerId	Specifies the owner of an NTR test, range of 1 to 32 alphanumeric characters.
TestName	Specifies the name of an NTR test, with a range of 1 to 32 alphanumeric characters.
TargetAddress	Specifies the target IPv4 address for the NTR test.
Dscp	Specifies the Differential Services Code Point (DSCP) value for use in packets that are generated by the NTR test. Range is 0 to 63. DEFAULT: 0
Attempts	Specifies the number of retries when a failure occurs Range is 1 to 10. DEFAULT: 2
Period	Specifies the inter-packet delay. Range is 10000 to 200000 microseconds. DEFAULT: 20000
AdminStatus	Specifies the administrator status. You must enable the administrator status to initiate the NTR test. DEFAULT: disabled
Label	Specifies the text label used to reference the NTR control entry. Range is 1 to 32 characters.

Viewing NTR test results

Use this procedure to view the results of an NTR test.

Procedure

1. From the navigation tree, double-click **Serviceability**.

2. In the **Serviceability** tree, double-click **SLA Monitor**.
3. In the **SLA Monitor** work area, click the **NTR** tab.
4. Click **Results**.
5. Click the **NTR Results Hidden** tab.

NTR Results Hidden field descriptions

Name	Description
OperStatus	Indicates the success or failure status of the NTR test. Values include: • inProgress : test results not yet available • aborted : indicates a general test failure occurred • completed
SrcAddress	Indicates source IPv4 address of the test packet.
SrcPort	Indicates the source UDP port of the test packet.
DstAddress	Indicates the destination UDP port of the test packet.
DstPort	Indicates the destination UDP port of the test packet.
Dscp	Indicates the DSCP value used in test packets.
TTL	Indicates the maximum TTL value used during test execution. The agent currently supports a maximum TTL of 32 for NTR tests. Generally speaking, a value of 32 indicates the TTL maximum was reached before the destination was reached.
HopCount	Indicates the number of hops maintained for the test.
AbortData	Indicates the reason for the failure of an NTR test execution.

Comments? infodev@avaya.com

Name	Description
CompletionData	Indicates the actual test results, at the protocol level, that are used by the test source to determine the overall test results (if available).
CompletionSummary	Provides a summary of the test results, i.e. test success (OK) or test failure (NA — No Response).

Viewing NTR per-hop test data

Use this procedure to view the per-hop test data as a result of a new trace route test.

Procedure

1. From the navigation tree, double-click **Serviceability**.
2. In the **Serviceability** tree, double-click **SLA Monitor**.
3. In the **SLA Monitor** work area, click the **NTR** tab.
4. Click **Results**.
5. Click the **NTR Results** tab.

NTR Results field descriptions

Name	Description
HopIndex	Indicates the index number associated with the hop:
TgtAddress	Indicates the IPv4 address of the test end station for the specified hop.
Rtt	Indicates the test round-trip-time for the specified hop in milliseconds.
IngressDscp	Indicates the DSCP value in the NTR test packet received by the test end station for the specified hop.
EgressDscp	Indicates the DSCP value in the NTR test response packet received by the SLAMon agent for the specified hop.

Executing RTP tests using EDM

Use this procedure to execute an RTP test on the network to establish QoS benchmark.

Before you begin

You must enable ServerBypass for the test to complete successfully.

About this task

Important:

When executing the script using EDM, do not run other commands while the script is in progress, because this slows down the execution. EDM can time-out while waiting for a response and even when a time-out occurs, the script execution continues on EDM.

Procedure

1. From the navigation tree, double-click **Serviceability**.
2. In the **Serviceability** tree, double-click **SLA Monitor**.
3. In the **SLA Monitor** work area, click the **RTP** tab.
4. In the toolbar, click **Insert**.
5. In the **OwnerId** field, type the owner id.
6. In the **TestName** field, type the test name.
7. In the **TargetAddress** field, type an IP address.
8. In the **Dscp** field, type the dscp value.
9. In the **TestPackets** field, enter a value.
10. In the **SyncPackets** field, enter a value.
11. In the **Period** field, enter a value.
12. In the **AdminStatus** section, select **enabled**.
13. In the **Label** field, enter a value.
14. Click **Insert** to initiate the RTP test.

Next steps

To view the test results, click **Results**.

Comments? infodev@avaya.com

RTP field descriptions

Name	Description
OwnerId	Specifies the owner of an NTR test, range of 1 to 32 alphanumeric characters.
TestName	Specifies the name of an NTR test, with a range of 1 to 32 alphanumeric characters.
TargetAddress	Specifies the target IPv4 address for the NTR test.
Dscp	Specifies the Differential Services Code Point (DSCP) value for use in packets that are generated by the NTR test. Range is 0 to 63. DEFAULT: 0
TestPackets	Specifies the number of packets used to determine end-to-end jitter. Range is 10 to 100. DEFAULT: 50
SyncPackets	Specifies the number of packets used to determine network delay. Range is 10 to 100. DEFAULT: 10
Period	Specifies the inter-packet delay. Range is 10000 to 200000 microseconds. DEFAULT: 20000
AdminStatus	Specifies the administrator status. You must enable the administrator status to initiate the RTP test. DEFAULT: disabled
Label	Specifies the text label used to reference the RTP control entry. Range is 1 to 32 characters.

Viewing RTP results

Use this procedure to view the results of a real time protocol test.

Procedure

1. From the navigation tree, double-click **Serviceability**.
2. In the **Serviceability** tree, click **SLA Monitor**.
3. In the **SLA Monitor** work area, click the **RTP** tab.

4. Click **Results**.

RTP Results field descriptions

Name	Description
OperStatus	Indicates the status of an RTP test. • **inProgess**: test is active • **aborted**: test has been stopped. Refer to AbortData for details. • **completed**: test is completed
SrcAddress	Indicates the source IP address used for the RTP test.
SrcPort	Indicates the port used for the RTP test.
DstAddress	Indicates the destination IP address used for the RTP test.
DstPort	Indicates the destination port used for the RTP test.
Dscp	Specifies the Differential Services Code Point (DSCP) value for use in packets that are generated by the RTP test.
AverageDelay	Indicates the average network delay (RTT) experienced during the RTP test execution in microseconds.
MedianDelay	Indicates the median network delay (RTT) experienced during the RTP test execution in microseconds.
PacketLoss	Indicates the count of packets lost during an RTP test execution.
OutOfOrderArrivals	Indicates the count of packets arriving out-of-order during an RTP test execution.
JitterQuartile0 – JitterQuartile4	Indicates the resulting quartile boundaries after sorting the network jitter values of all test packets during the RTP test execution. The value is represented in microseconds.

Comments? infodev@avaya.com

Name	Description
AbortData	Indicates the details of the RTP test that was aborted. Values can include more than one of the following: • **other** • **agentDisabled** • **agentBusy** • **timeout** • **cancelled** • **deniedByTarget** • **networkIssue** • **timeSync**

Comments? infodev@avaya.com

Index

Numerics

1..64 field 123
1024..1518 field 123
128..255 field 123
256..511 field 123
511..1023 field 123
65..127 field 123

A

Absolute statistic 137
ActiveOpen 115
AddrMaskReps field 113, 114
AddrMasks field 113, 114
alarms, RMON 16, 18
    characteristics of 16
    creating 18
AlignmentErrors field 119, 132
AttemptFails 115
AuthEapLogoffWhileAuthenticated field 126
AuthEapLogoffWhileAuthenticating field 126
AuthEapStartsWhileAuthenticated field 126
AuthEapStartsWhileAuthenticating field 126
AuthFailWhileAuthenticating field 126
AuthReauthsWhileAuthenticated field 126
AuthReauthsWhileAuthenticating field 126
AuthSuccessWhileAuthenticating field 126
AuthTimeoutsWhile Authenticating field 126
Average per sec statistic 137

B

BackendAccessChallenges field 126
BackendAuthFails field 126
BackendAuthSuccesses field 126
BackendNonNakResponsesFromSupplicant field 126
BackendOtherRequestsToSupplicant field 126
BackendResponses field 126
Bridge tab 121
BroadcastPkts field 123, 137, 143
buckets 140
BucketsGranted field 140
BucketsRequested field 140, 141

C

CarrierSenseErrors field 119, 132
Chassis ICMP In statistics window 112
Chassis ICMP Out statistics tab 113
Collisions field 123, 137, 143
Community field 149, 151
config field 56
Configuring RMON with the ACLI 69
CRCAlignErrors field 123, 137, 143
Creating a graph 108
critical field 56
Cumulative statistics 137
CurrEstab 115

D

DeferredTransmissions field 119, 132
DelayExceededDiscards field 122
Description field 149, 151
DestUnreachs field 113, 114
DropEvents field 143

E

EapLengthErrorFramesRx field 125
EapLogoffsWhileConnecting field 126
EAPOL 124, 125
EAPOL Diag tab 125
EAPOL Stats tab 124
EapolFramesRx field 125
EapolFramesTx Field 125
EapolLogoffFramesRx field 125
EapolReqFramesTx field 125
EapolReqIdFramesTx field 125
EapolRespFramesRx field 125
EapolRespIdFramesRx 125
EapolStartFramesRx field 125
EchoReps field 113, 114
Echos field 113, 114
EntersAuthenticating field 126
EntersConnecting field 126
EstabResets 115
Ethernet statistics, disabling 144
events, RMON 149
ExcessiveCollisions field 119, 132

F

falling event 149
Falling Event Index field 145
Falling Threshold field 145
falling value, RMON alarms 16
FallingEventIndex field 147
FallingThreshold field 147
FCSErrors field 119, 132
ForwDatagrams field 111
FragCreates field 111
FragFails field 111
Fragments field 137, 143
FragOKs field 111
FrameTooLongs field 119, 132

G

Graphing multilink trunk statistics 130
Graphing switch chassis data 108
Graphing switch port data 117
Graphing VLAN DHCP statistics 135

H

HCInBroadcastPkt field 131
HCInMulticastPkt field 131
HCInOctets field 131
HCInUcastPkts field 131
HCOutBroadcast field 131
HCOutMulticast field 131
HCOutUcastPkts field 131
HDOutOctets field 131

I

ICMP Out statistics 113
ifOutOctets field 117
IGMP and the system event log 19
InAddrErrors field 111
InASNParseErrs field 109
InBadCommunityNames field 109
InBadCommunityUses field 109
InBadValues field 109
InBadVersions field 109
InBroadcastPkt field 131
InDatagrams 116
InDelivers field 111
Index field 145
InDiscards field 111, 117, 122
InErrors 116
InErrors field 117
inErrs 115
InFrames field 122
InGenErrs field 109
InGetNexts field 109
InGetRequests field 109
InGetResponses field 109
InHdrErrors field 111
InMulticastPkts field 131
InNoSuchNames field 109
InNUcastPkts field 117
InOctets field 117
Inpkts field 109
InReadOnlys field 109
InReceives field 111
InSegs 115
InSetRequests field 109
InternalMacReceiveErrors field 119, 132
InternalMacTransmitErrors field 119, 132
Interval field 140, 141, 145, 147
InTooBigs field 109
InTotalReqVars field 109
InTotalSetVars field 109
InUcastPkts field 117
InUnknownProtos field 111, 117
InvalidEapolFramesRx field 125

J

Jabbers field 123, 137

L

Last sec statistic 137
LastTimeSent field 149
LateCollisions field 119, 132
logs 152

M

Max per sec statistic 137
Min per sec statistic 137
MtuExceededDiscards field 122
MulticastPkts field 123, 137, 143
MultipleCollisionFrames field 119, 132

N

NoPorts 116

O

Octets field 123, 137, 143
OutBadValues field 109
OutBroadcast field 131
OutDatagrams 116
OutDiscards field 111, 117
OutErrors field 117
OutFrames field 122
OutGenErrs field 109
OutMulticast field 131
OutNoRoutes field 111
OutNoSuchNames field 109
OutNUcastPkts field 117
Outpkts field 109
OutRequests field 111
OutRsts 115
OutSegs 115
OutTooBigs field 109
OutTraps field 109
OutUcastPkts field 117
OversizePkts field 123, 137, 143
Owner field 140, 141, 144, 147, 149, 151

P

ParmProbs field 113, 114
PassiveOpens 115
Pkts field 123, 137, 143
port Ethernet Error Statistics tab 119
Port field 144
Port mirroring 21
ports 117
    graphing 117

R

ReasmFails field 111
ReasmOKs field 111
ReasmReqds field 111
Redirects field 113, 114
Remote logging 15
Remote Monitoring,See RMON 32
RetransSegs 115
rising event 149
Rising Event Index field 145
Rising Threshold field 145
rising value, RMON alarms 16
RisingEventIndex field 147
RisingThreshold field 147
RMON 16, 18, 137, 140–142, 145, 149
    alarms 16, 18, 145
    graphing 137
    alarms 16, 18, 145
        characteristics 16
        creating 18
    events 149
        definition 149
    history 140–142
        creating 141
        definition 140
        disabling 142
    statistics 137, 141

S

Sample Type field 145, 147
SampleIndex field 143
serious field 56
SingleCollisionFrames field 119, 132
SQETestErrors field 119, 132
SrcQuenchs field 113, 114
stack loopback test 28
stack monitor 29
StartupAlarm field 147
statistics 113, 137, 141
    ICMP Out 113
    RMON 137, 141
Status field 147
support 12
    contact 12
System logging 15

T

test 28
    stack loopback 28
TimeExcds field 113, 114
TimestampReps field 113, 114
Timestamps field 113, 114
Type field 149, 151

U

UndersizePkts field 123, 137, 143
Utilization field 143

V

Value field 147
Variable field 145, 147
videos 11