Configuring System Monitoring on Avaya Ethernet Routing Switch 4000 Series

Release 5.7
NN47205-502
Issue 09.02
March 2015

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 You 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 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 products, 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.

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.

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.

Contents

Chapter 1: Introduction

Related Links

Purpose on page 9
Related resources on page 9
Support on page 11

Purpose

This document provides system monitoring concepts and procedures for the Avaya Ethernet Routing Switch 4000 Series.

Related Links

Introduction on page 9

Related resources

Documentation

For a list of the documentation for this product, see *Documentation Reference for Avaya Ethernet Routing Switch 4000 Series*, NN47205–101.

Training

Ongoing product training is available. For more information or to register, see http://avaya-learning.com/.

Enter the course code in the **Search** field and click **Go** to search for the course.

Course code	Course title
8D00020E	Stackable ERS and VSP Products Virtual Campus Offering

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

Procedure

- 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.

Searching a document collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx, for example, ers4000_5.7x.pdx.
3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
   - Whole words only
   - Case-Sensitive
   - Include Bookmarks
   - Include Comments
6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance ranking.

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.

Related Links

Introduction on page 9

Chapter 2: New in this release

The following sections detail what is new in *Configuring System Monitoring on Avaya Ethernet Routing Switch 4000 Series*, NN47205-502 for Release 5.7.

Features

See the following sections for information about feature changes.

SLA Monitor

The Service Level Agreement (SLA) Monitor feature is implemented phase-wise on the ERS 4000 series switch. In Release 5.6, the phase 1 implementation included the feature, SLA Monitor on the ERS 4000 series switch and supported only non-secure agent-server communication.

In Release 5.7, phase 2 implementation ensures a secure SLA Monitor agent-server communication through certificate-based authentication and encrypted agent-server communication. Also, SLA Monitor agent can perform QoS tests in the absence of SLA Monitor server using the platform CLI.

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.

For more information about SLA Monitor agent, see

- SLA Monitor on page 33
- SLA monitor configuration using ACLI on page 89
- SLA Monitor configuration using EDM on page 160

.

Remote Switch Port ANaylzer

Remote Switch Port ANalyzer (RSPAN), also known as Remote Port Mirroring, enhances port mirroring by enabling mirroring traffic to be sent to one or more switches or stacks on the network using an intermediate VLAN for forwarding the mirrored traffic.

For more information, see

- RSPAN on page 25
- RSPAN interactions with other features on page 27
- Configuring Many-to-Many port-mirroring using ACLI on page 60
- Configuring an RSPAN source session using ACLI on page 63
- Configuring an RSPAN destination session using ACLI on page 65
- Displaying RSPAN information on page 66
- Configuring an RSPAN source session using EDM on page 100
- Configuring an RSPAN destination session using EDM on page 102

Trace feature

The trace feature is a troubleshooting feature that provides detailed information about errors and events on the device. Use this feature to understand the cause of an error and take action to resolve it. The trace feature provides more detailed, real time information than a **`show`** command.

For more information, see

- System diagnostics and statistics using ACLI on page 45
- Trace diagnosis of problems on page 45
- Trace diagnosis of problems navigation on page 45
- Using trace to diagnose problems on page 45

Other changes

See the following section for information about changes that are not feature-related.

New Introduction chapter

The Introduction chapter replaces the Purpose of this document and Customer service chapters

Chapter 3: System monitoring fundamentals

System monitoring is an important aspect of switch operation. The switch provides a wide range of system monitoring options that the administrator can use to closely follow the operation of a switch or stack.

This chapter describes two general system monitoring considerations, system logging and port mirroring, for the switch. Subsequent chapters provide information about specific system monitoring tools and their use.

CPU and memory utilization

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

The memory utilization provides you information on what percentage of the dynamic memory is currently used by the system. The switch displays memory utilization in terms of megabytes available since system bootup.

This feature does not require a configuration. It is a display-only feature.

Light Emitting Diode (LED) on the Avaya Ethernet Routing Switch 4000 Series

The Avaya Ethernet Routing Switch 4000 Series displays diagnostic and operation information through the LEDs on the unit. Familiarize yourself with the interpretation of the LEDs on the 4000 series device. For detailed information regarding the interpretation of the LEDs, see *Installing Avaya Ethernet Routing Switch 4000 Series*, NN47205-300.

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, alleviating the network manager from querying each switch individually to interrogate the log files.

You must configure the remote syslog server to log informational messages to this remote server. The User Datagram Protocol (UDP) packet is sent to port 514 of the configured remote syslog server.

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, the system stores up to 10 messages that are sent after the IP address of the remote server is on the system.

You can configure this feature by enabling remote logging, specifying the IP address of the remote syslog server, and specifying the severity level of the messages to be sent to the remote 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. See Configuring remote system logging using EDM on page 141

SNMP traps

SNMP traps are configured as notification controls. For more information about notification controls, see *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.

MIB 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:

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

IGMP and the system event log

Internet Group Management Protocol (IGMP) uses the components provided by the syslog tool. Functions such as storing messages in the Non-volatile Random Access Memory (NVRAM) or remote host, and displaying these log messages through the ACLI or Telnet is then carried out by the syslog tool on its own.

The IGMP log events can be classified into the following three categories based on their severity:

- critical
- serious
- informational

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

- IGMP initialization
- configuration changes
- Stack join events
- IGMP messages: report, leave, and query messages received by the switch

Important:

Events such as reception of IGMP messages happen frequently in the switch, whenever a new host joins or leaves a group. Logging such messages consumes a lot of log memory. Therefore, such messages should not be logged all the time. By default, logging of such messages is disabled. You must enable this feature through the ACLI.

In the table Table 1: IGMP syslog messages on page 16:

- %d represents a decimal value for the parameter preceding it, for example, 5 for Virtual Local Area Network (VLAN) 5
- %x represents a hexadecimal value for the parameter preceding it, for example, 0xe0000a01 for Group 224.0.10.1

The following table describes the IGMP syslog messages and their severity.

Table 1: IGMP syslog messages

Severity	Log Messages
Informational	IGMP initialization success
Critical	IGMP initialization failed: Error code %d
Informational	IGMP: policy initialization success
Informational	IGMP:policy initialization failed
Informational	IGMP configuration loaded successfully
Informational	IGMP configuration failed: Loaded to factory default

Table continues…

Severity	Log Messages
Informational	IGMP: Version %d Snooping enabled on VLAN %d
Informational	IGMP: Version %d Snooping disabled on VLAN %d
Informational	IGMP: Proxy enabled on VLAN %d
Informational	IGMP: IGMP version %d enabled on VLAN %d
Informational	IGMP: IGMP version %d disabled on VLAN %d
Informational	IGMP: 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 disabled
Informational	IGMP: Added reserved multicast address
Informational	IGMP: Removed reserved multicast address
Informational	IGMP: Unable to add reserved multicast address
Informational	IGMP: Exceeded reserved multicast address range: #Addr %d * #VLANs %d > %d
Informational	IGMP configuration changed: Trunk %d created for IGMP
Informational	IGMP: Trunk %d created. IGMP groups added on all trunk ports
Informational	IGMP configuration changed: Trunk %d removed for IGMP ports
Informational	IGMP: Trunk %d removed. IGMP groups removed on all trunk 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: Dynamic router port %d added
Informational	IGMP: Dynamic router port %d removed
Informational	IGMP: Config. database sent by unit %d
Informational	IGMP: Config. database received on unit %d from %d
Informational	IGMP: Config database exchanged between all units of the stack
Informational	IGMP: Error sending database from unit %d
Informational	IGMP stack join completed. Database synchronized
Serious	IGMP not able to join stack: Error code %d
Informational	IGMP: Group database sent by unit %d
Informational	IGMP Group database received on unit %d from %d
Informational	IGMP: Group database received from all non-base units
Informational	IGMP: Error sending group database from unit %d

Table continues…

Severity	Log Messages
Informational	IGMP: REPORT received for Group %s on VLAN %d and port %d
Informational	IGMP: LEAVE received for Group %s on VLAN %d and port %d
Informational	IGMP: QUERY received on port %d

Stack Monitor

You use the Stack Monitor feature to analyze the health of a stack by monitoring the number of active units in the stack.

With stacked switches, multilink trunking (MLT) links are often connected to separate units in a distributed MLT (DMLT). If the connections between switches in the stack fail, a situation can arise where the DMLT links are no longer connected to a stack, but to a combination of units that are no longer connected to each other. From the other end of the DMLT, the trunk links appear to be functioning properly. However, the traffic is no longer flowing across the cascade connections to all units, so the connectivity problems can occur.

With the Stack Monitor feature, when a stack is broken, the stack and any disconnected units from the stack, send Simple Network Management Protocol (SNMP) traps. If the stack or the disconnected units are still connected to the network, they generate log events and send trap messages to the management station to notify the administrator of the event. After the problem is detected, the stack and disconnected units continue to generate log events and send traps at a user-configurable interval until the situation is remedied (or the feature is disabled).

Local ports shutdown while stacking

When a switch is joining the stack, DMLT and dynamic Link Aggregation Groups (LAG) formed with Link Aggregation Protocol (LACP) can still be created because Link Layer Discovery Protocol Data Units (LACPDU) continue to be transmitted. This results in a temporary traffic delay (for a few seconds) until the switch fully joins the stack.

Release 5.2 software resolves this issue by momentarily shutting down the local ports on a switch before the switch joins the stack. After a reset or power up, if the switch detects power on its stacking cables and is connected to another unit, the switch shuts down all of its local ports. When the ports are disabled, the port LEDs blink, similar to ports that are shut down. The ports are reenabled when the unit finishes entering the stack formation or after a 60-second timeout, whichever comes first.

If the unit does not detect power on the stacking ports 20 seconds after it comes up, the local ports forward the traffic.

Stack loopback test

The stack loopback test feature allows the customer to quickly test the switch stack ports and the stack cables on 4000 units. This feature helps you while experiencing stack problems to determine whether the root cause is a bad stack cable or a damaged stack port and prevents potentially good switches being returned for service. You can achieve this by using two types of loopback tests:

- Internal loopback test
- External loopback test

Caution:

For accurate results, run the internal loopback test before the external loopback test.

Internal loopback test

Use the internal loopback test by putting each of stack links in loopback mode one by one, sending 1000 packets, and verifying that the packets are received back with the same content.

The purpose of the internal loopback test is to verify that all the stack ports are functional.

External loopback test

Use the external loopback test by connecting the stack uplink port, with the stack downlink port, sending 1000 packets from the uplink port and verifying that the packets are received back on the downlink port. The same tests are done by sending the packets from the downlink port and verifying that they are received back on the uplink port. The purpose of the external loopback test is to verify that the stack cable is functional.

Run the internal test before the external test and before the stack ports are verified to be functional.

On known good units and stack cables, no errors are returned by the internal and the external loopback test. The external loopback test returns an error if the stack cable is not present.

The main limitation of this feature is that it interferes with the normal functioning of the stack manager. Therefore, you must run both the tests on units that are taken off the stack.

Important:

Hardware Limitation: This feature is only useful for stackable switches.

Software Limitation: You can execute only one test at a time. If a test is started and not finished, a second test cannot be started until the first stops.

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.

Stack Health Check

You can use Stack Health Check to:

- provide information on the stacking state of each switch rear port
- run a high-level test to monitor the rear port status for each unit
- confirm the number of switching units in stack
- detect whether the stack runs with a temporary base unit
- monitor the stack continuity

By default, the health check is enabled on all the stack units. You can use Stack Health Check in both user interfaces: ACLI and EDM.

Port mirroring

You can designate a switch port to monitor traffic in the following ways:

- on any two specified switch ports, port-based
- to or from any two specified addresses that the switch learns, address-based

You must connect an Ethernet monitoring device to the designated monitor port to connect the mirrored traffic.

When you enable Port-Mirroring with one of the following modes, higher available precedence will be used for all ports:

- Asrc
- Adst
- AsrcBdst
- AsrcBdstOrBsrcAdst
- AsrcOrAdst
- XrxYtxOrYrxXtx
- XrxYtx

Important:

You cannot free resources used by Port Mirroring with the **`qos agent reset-default`** command

If a unit leaving the stack causes invalid port-mirroring instances or RSPAN destination instances, these instances will not be displayed in the ASCII running config file. The `show port-mirroring [rspan]` command output indicates invalid RSPAN or port-mirroring instances by marking them with an asterisk (*) character after the instance number.

The output may vary from unit to unit, for the same instance. For example, consider a port-mirroring instance with all configured ports residing on unit 2. When unit 2 leaves the stack, this instance becomes invalid on stack but remains valid on unit 2.

Note:

Each of the XrxorXtx, XrxOrYtx, ManyToOneRxTx modes needs twice the hardware resources of a usual port mirroring instance. This means whenever you use one or more of these modes, instead of configuring up to four port-mirroring instances, you can only configure up to:

- two instances, if both instances are of type XrxorXtx or XrxOrYtx or ManyToOneRxTx, in any combination
- three instances if one, and only one, of these instances is of type XrxorXtx or XrxOrYtx or ManyToOneRxTx

If your configured port-mirroring instances exceed hardware resources (for example, when you configure one XrxorXtx, one ManyToOneRxTx and one asrc instance), an error message is generated: "Not enough HW resources are available".

Many-to-Many Port Mirroring

You can use the many-to-many port mirroring feature to configure multiple sessions of mirroring configurations, each with a monitor port and mirrored ports.

You can provide a way to monitor more than one traffic pattern by using many-to-many port mirroring. You can use this feature to monitor multiple traffic patterns, which is important in networks which support a variety of complex user scenarios. As an example, you can set up port mirroring to

allow duplication of VoIP traffic for call recording, another instance for intrusion detections, and still another instance for other activities or network troubleshooting.

You can configure this feature by using ACLI or EDM. To configure each instance, you follow the same configuration process as the 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.

Address-based modes

The following address-based modes are supported:

- 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 limitations and restrictions

You can use many-to-many port mirroring on both pure stacks and standalone boxes.

You cannot configure a monitor port (MTP) that is a mirrored port for another MTP. Frames mirrored to one MTP are not taken into account in MAC address-based mirroring on another MTP.

If you configure a port to be egress-mirrored in one instance, then that port cannot be egress-mirrored in another instance (to another MTP). Similarly, if you configure a port to be ingress-

mirrored, then the system prohibits that port to be ingress-mirrored in another instance. The system allows a port to be ingress-mirrored in one instance and egress-mirrored in another.

The ports you configure as monitor ports may be allowed to participate in normal frame switching operation or be used as management ports, provided that you enable port mirroring with the allow traffic option.

You can configure up to four monitor ports.

You can configure multiple instances by using the existing interface in ACLI or EDM. The system attaches one monitor port (MTP) to each instance. In some cases a monitor port can be used in more than one instance.

You cannot configure a port as a monitor port if it exists as part of an MLT group.

For MAC base modes: Asrc, Adst, AsrcBdst, AsrcBdstOrBsrcAdst, AsrcOrAdst and port based modes: XrxYtx, XrxYtxOrYrxXtx port-mirroring, you need to install filters to enable port mirroring. The application may not function in these modes if platform resource limits are reached.

Port-based mirroring configuration

Figure 1: Port-based mirroring example on page 23 shows an example of a port-based mirroring configuration in which port 44 is designated as the monitor port for ports 45 and 46 of Switch S1. Although this example shows ports 45 and 46 monitored by the monitor port (port 44), you can monitor any of the trunk members of T1 and T2.

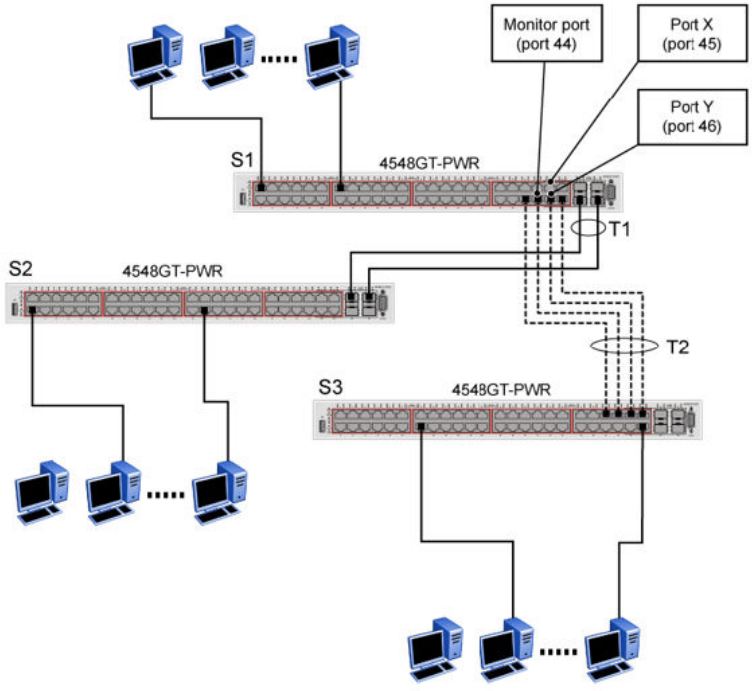


Figure 1: Port-based mirroring example

This example 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.

Important:

You cannot configure trunk members as monitor port.

In the configuration example shown in the preceding figure, you can set the designated monitor port (port 44) 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/transmitted by port X and transmitted/received by port Y (conversations between port X and port Y).
- Monitor all traffic received on many ports (ManytoOneRX).
- Monitor all traffic transmitted on many ports (ManytoOneTX).
- Monitor all traffic received or transmitted on many ports (ManytoOneRxTX).

Address-based mirroring configuration

The following figure shows an example of an address-based mirroring configuration in which port 44, the designated monitor port for Switch S1, monitors traffic occurring between address A and address B.

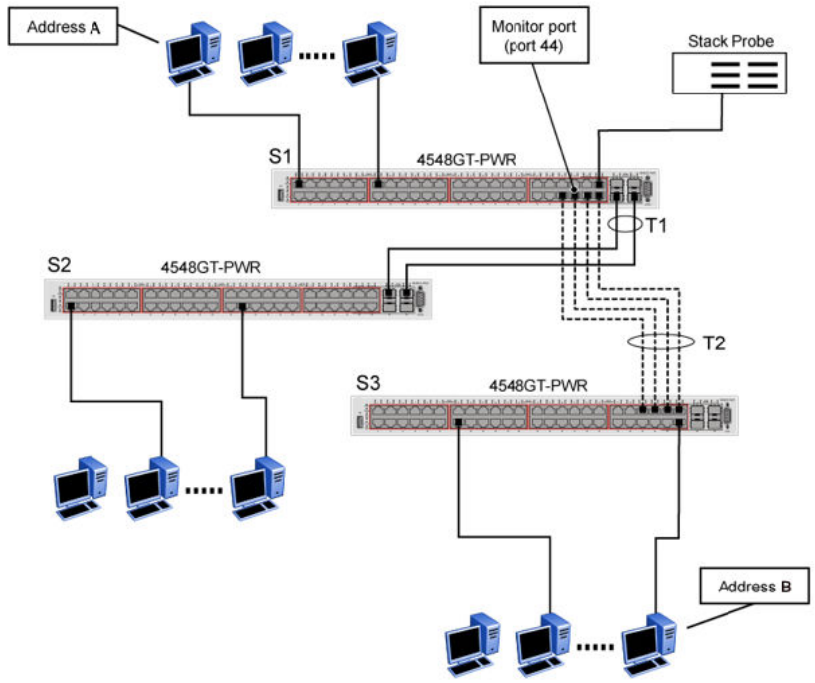


Figure 2: Address-based mirroring example

In this configuration, you can set the designated monitor port (port 44) 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).

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 on the 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:

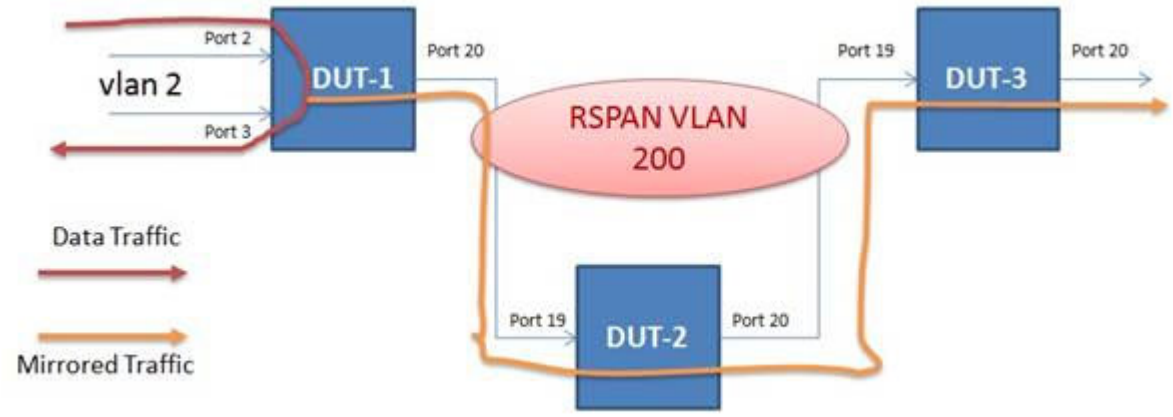
On an intermediate switch, Avaya recommends that you configure up to 12 ports.

Note:

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

ERS 4500 cannot function as an RSPAN intermediate switch.

The following figure shows how the RSPAN is working for three connected devices:



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

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

Port-mirroring interactions

- 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 Remote Port Mirroring with MAC base modes Asrc, Adst, AsrcBdst, AsrcBdstOrBsrcAdst, AsrcOrAdst, and port based modes XrxYtx, XrxYtxOrYrxXtx, you must install filters to enable an RSPAN source session. If platform resource limits are reached, the application may not function in these modes.
- For port based modes XrxYtx and XrxYtxOrYrxXtx, RSPAN can function only for unicast traffic.
- The RSPAN destination port is set as an untagged member of the RSPAN VLAN, to ensure that the RSPAN tag is stripped off.
- Mac-security cannot be enabled on RSPAN destination-ports, because a destination port is also a monitor port.

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.

IPFIX

With IP Flow Information Export (IPFIX) you can monitor traffic flows by configuring observation points to collect flow statistics over a designated time period.

IPFIX supports the following external IPFIX collectors:

- NetQoS Harvester/Collector

- Avaya IP Netflow Version 9
- Avaya IP Flow Manager
- Fluke Collector

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

- protocol type
- destination IP address
- source IP address
- ingress port
- type of service (TOS)

You cannot use IPFIX on secondary interfaces.

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

- source port
- destination port

Beginning with Release 5.4, the Avaya Ethernet Routing Switch 4000 supports IPFIX through the following:

- the creation and display of sampled information
- the ability to export this sampled information

Note:

IPFIX also monitors IGMP traffic.

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 *Configuring Quality of Service on Avaya Ethernet Routing Switch 4000 Series*, NN47205-504.

Remote Network Monitoring (RMON)

The Remote Network Monitoring (RMON) Management Information Base (MIB) is an interface between the RMON agent on the switch and an RMON management application, such as the Enterprise Device Manager (EDM).

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

The RMON agent continuously collects statistics and proactively monitors switch performance.

RMON has the three following major functions:

- to create and display alarms for user-defined events
- to gather cumulative statistics for Ethernet interfaces
- To track the history of statistics for Ethernet interfaces

RMON scaling

The number of RMON alarm instances per stack has increased from 400 to 800 with release 5.2 for the Avaya Ethernet Routing Switch 4000 series products.

Working of RMON alarms

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

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

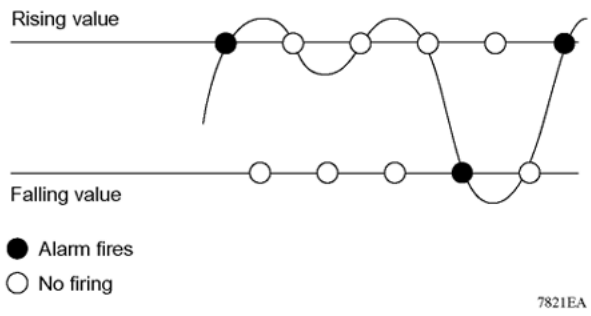


Figure 3: How alarms fire

It is important to note that the alarm triggers 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 the system administrator when 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 the notification you need if the lower limit of octets going out is defined at 260 and the upper limit is defined at 320 (or at any value greater than 260 + 52 = 312).

The first time outbound traffic other than spanning tree Bridge Protocol Data Units (BPDU) occurs, the rising alarm triggers. When outbound traffic other than spanning tree ceases, the falling alarm triggers. This process provides the system administrator with time intervals of any nonbaseline outbound traffic.

You define the alarm with a falling threshold less than 260 (assuming the alarm polling interval is 10 seconds), say 250, the rising alarm can fire only once (see the following figure). For the rising alarm to fire a second time, the falling alarm (the opposite threshold) must fire. Unless the port becomes inactive or spanning tree is disabled (which causes the value for outbound octets to drop to zero), the falling alarm cannot fire because the baseline traffic is always greater than the value of the falling threshold. By definition, the failure of the falling alarm to fire prevents the rising alarm from firing a second time.

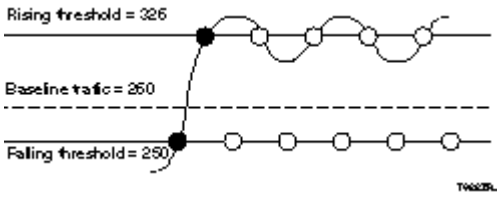


Figure 4: Alarm example - threshold less than 260

Creating alarms

When you create an alarm, select a variable from the variable list and the 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.

When 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 an as absolute value. Therefore, an alarm can be created with a rising value of 2 and a falling value of 1 to alert a user about whether the card is up or down.

Note:

When you configure an RMON alarm with an owner, the system does not retain the owner configuration after reboot and the system displays the owner as "Entry from NVRAM".

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 given delta-valued alarm and add them together the result is twice the actual value. (This result is not an error in the software.)

RMON events and alarms

RMON events and alarms work together to produce notification when values in the network go out of a specified range. When values pass the specified ranges, the alarm is triggered. The event specifies how the activity is recorded.

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

- Rising Event
- Falling Event

Default events specify that when an alarm goes out of range, the firing of the alarm is tracked in both a trap and a log. For example, when an alarm triggers at the rising threshold, the rising event specifies that this information be sent to both a trap and a log. You can enable the viewing of the history of RMON fault events by using the stack. RMON Event Log window

How events work

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

- RisingEvent
- FallingEvent

The default events specify that when an alarm goes out of range, the firing of the alarm is tracked in both a trap and a log. For example, when an alarm triggers at the rising threshold, the rising event specifies that this information be sent to both a trap and a log. Likewise, when an alarm passes the falling threshold, the falling event specifies that this information is sent to a trap and a log.

Show Environmental

This feature provides an enhancement to display environmental information about the operation of the switch or units within a stack. The Show environmental command does not require any specific configuration, and it reports the following parameters for each switch:

- power supply status
- fan status
- switch system temperature

The Show Environmental command depends on the hardware of each unit. The command is available from any ACLI mode, and you do not need to enable or activate this feature. The

command displays information for a stand-alone switch and for each unit in a stack, regardless of how many units are in that stack.

You can configure the Show Environmental command in ACLI, SNMP, and EDM.

The following table defines the various states of the environment of a switch.

Table 2: Environmental parameters

Measurement	State	Description
PSU1	Primary	If the power source is present and is the primary power source
PSU2	Redundant	If the power source is present and is the redundant power source
	N/A	If the power source is missing or not providing power
Fan	OK	If the fan is working properly
	FAIL	If any fan malfunction exists
	N/A	If the fan dose not exist
Temperature	OK	If temperature is lower than 40C
	HIGH	If temperature is greater than 40C

SLA Monitor

The Avaya ERS 4000 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

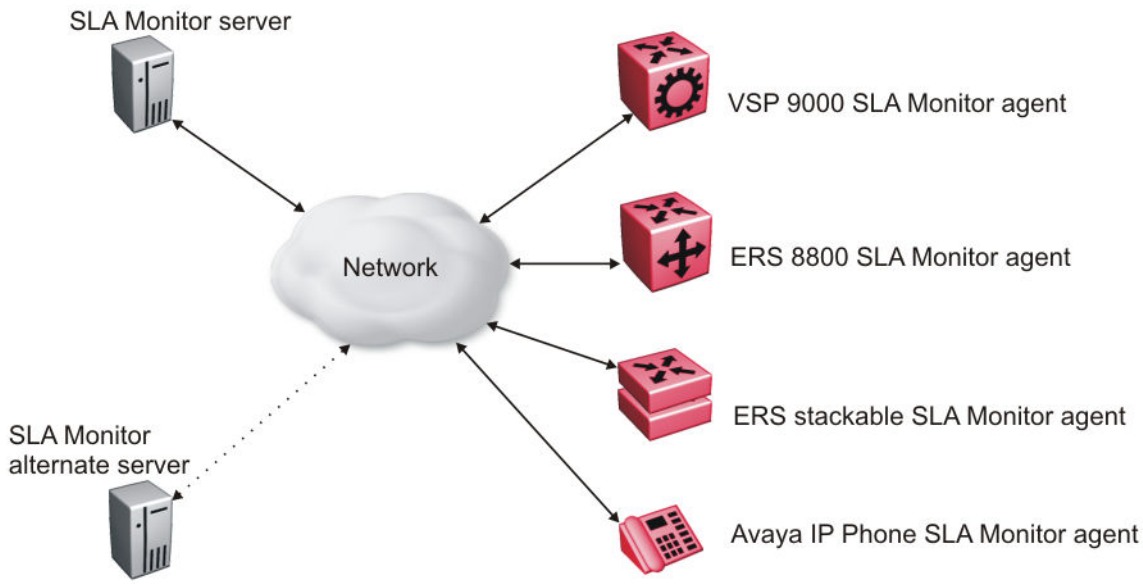
SLA Monitor agent performs QoS tests after it receives a request from the SLA Monitor server. The tests can be performed even if the server is not available.

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 time-out 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 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.

You can use NTR and RTP to perform the following tests in the absence of an SLA Monitor server:

- You can access the SLA Monitor CLI through the SLAMon Agent Address SLAMon Agent Port. By default, access to the SLA Monitor CLI interface is disabled. If access is enabled, the SLA Monitor CLI interface becomes available when the SLA Monitor agent is enabled. Tests are run serially and only one type of test can be run at a time. Established sessions time-out after a specified interval. The time interval can be 60 seconds to 600 seconds. By default, the interval is 60 seconds. You can disable the SLA Monitor CLI interface if the functionality is not required.
- You can run the NTR and RTP tests through the ACLI using the Application Configuration mode. The SLA Monitor agent must be enabled. Tests are run serially and only one type of test can be run at a time.

Note:

Server bypass must be enabled on the agents that are not registered with the server but are target agents for the RTP tests.

The error message “Unable to initiate test - agent busy” or “Reported Issue: test request denied by remote agent” appears if any tests are executed during the same time when the tests initiated by the server are executed. The server initiated tests typically takes priority. Do any one of the following if the error message appears:

- Stop the server
- Enable SLAMon Agent Refuse Server Tests on the remote agent

Note:

Command execution fails if you disable the SLA Monitor agent.

Limitations

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

Chapter 4: Network monitoring configuration using ACLI

This chapter describes the ACLI commands that you use to configure network monitoring using the ACLI

Viewing CPU utilization using ACLI

Use this procedure to view the CPU utilization of the switch or stack.

Procedure steps

1. Access the Privileged exec mode.
2. Enter the following command:

```
show cpu-utilization
```

Job Aid

The following figure is an example of CPU utilization output.

```
4526GTX-PWR (config)#show cpu-utilization
--------------------------------------------------------------
        CPU Utilization
--------------------------------------------------------------

Unit/ Last 10 Sec, 1 Min, 10 Min, 60 Min, 24 Hrs, System Boot-Up
--------------------------------------------------------------
1       25%   25%   24%   NA    NA    26%
2       24%   24%   24%   NA    NA    25%
```

Viewing memory utilization using ACLI

Use this procedure to view the memory utilization of the switch or stack.

Procedure steps

1. Access the Privileged exec mode.
2. Enter the following command:

```
show memory-utilization
```

Job Aid

The following figure is an example of memory utilization output.

```
4526GTX-PWR(config)#show memory-utilization
---------------------------------------
      Memory Utilization
---------------------------------------
Unit/ Total     Used        Free
---------------------------------------
1  128Mbytes    75 Mbytes    53 Mbytes
2  128Mbytes    75 Mbytes    53 Mbytes
```

Viewing system logging information using ACLI

Use this procedure to display system logging configuration information.

Prerequisites

- Log on to the Privileged EXEC mode in ACLI.

Procedure steps

1. To view system logging information, enter the following command :

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

Variable definitions

The following table defines parameters that you can enter with the `show logging [config] [critical] [informational] [serious] [sort-reverse] [unit <1-8>]` command.

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

Job aid: show logging config command output

The following table displays sample output for the **`show logging config`** command.

```
ERS4000(config)# show logging config
Event Logging: Enabled
Volatile Logging Option: Latch
Event Types To Log: Critical, Serious, Informational
Event Types To Log To NV Storage: Critical, Serious
Remote Logging: Enabled
Remote Logging Address: 4000:52:3:4:5:6:7:2
Remote Logging Address: 172.16.2.2
Event Types To Log Remotely: None
```

Configuring syslog capabilities using ACLI

Use this procedure to display and clear the last software exception

Procedure steps

1. Access the Priv Exec mode.

2. To display the last software exception, enter the following command:

   ```
   show system last-exception [unit{<1-8>|all}]
   ```

3. To clear the last software exception, enter the following command:

   ```
   clear last-exception [unit{<1-8>|all }]
   ```

Variable definitions

Variable	Value
unit <1-8> | all	The unit specified for the command. If you do not specify a unit, the last unit the command was run on is used.

Job Aid

The following figure shows the output for the show system last-exception unit command.

```
  Last Saved Exception - Unit# 2
------------------------------

bld version: 1.0.26.0 time: (26/Jan/07 18:29:26) view: (icatana_b)
sysUpTime: 104511 Registers:

     R00      R01      R02      R03      R04      R05      R06      R07
9866cc05 555f9000 00000000 00000000 00000000 00000000 00000000 00000000
     R08      R09      R10      R11      R12      R13      R14      R15
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
     R16      R17      R18      R19      R20      R21      R22      R23
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
     R24      R25      R26      R27      R28      R29      R30      R31
00000000 00000000 00000000 00000000 00000000 00000000 60531c00 0000021b

Exception type: Data Access
Task Name "tFault"
  KrnlSt 0, IntCnt 0, TskLckCnt 0, DAR 0x00000000, PC 0x0075c924, SP 0x037f8b80
- Exception Stack Trace
  + PC 0x005c0074
  + PC 0x8728037f
  + PC 0x6f900000
= Total 192 Bytes =
```

Configuring system logging using ACLI

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

Procedure steps

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

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

Variable definitions

Variable	Value
enable | disable	Enables or disables the event log (enabled is the default setting).
level critical | serious | informational | none	Specifies the level of logging stored in Dynamic Random Access Memory (DRAM).
nv-level critical | serious | none	Specifies the level of logging stored in NVRAM.
remote	Configures remote logging parameters. Address: configure remote syslog address. Enable: enable remote logging. Level: configure remote logging level.
volatile	Configures options for logging to DRAM. Latch: latch DRAM log when it is full. Overwrite: overwrite DRAM log when it is full.

Disabling logging using ACLI

You can use the following procedure to disable the system event log

Procedure steps

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

```
no logging
```

Default logging using ACLI

Configure the system settings as the factory default settings for the system event log.

Procedure steps

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

```
default logging
```

Clearing log messages using ACLI

You can use the **`clear logging`** command to clear all log messages in DRAM.

Procedure steps

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

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

Variable Definitions

The following table describes the command parameters.

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

Configuring remote system logging using ACLI

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

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

To configure the remote system log, enter the following command:

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

Variable definitions

The following table defines parameters that you can enter with the **`logging remote [address <A.B.C.D|WORD>] [secondary-address <A.B.C.D|WORD>] [enable] [level <critical|informational|none|serious>] [facility <daemon|local0|local1|local2|local3|local4|local5|local6|local7>]`** 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. Value is a character string with a maximum of 45 characters.
`secondary-address <A.B.C.D|WORD>`	Specifies the secondary remote system log server IP address. • A.B.C.D—the IPv4 address of the remote server • WORD—the remote host IPv6 address. Value is a character string with a maximum of 45 characters.
`enable`	Enables system message logging on the remote server. You must configure either the primary or secondary remote server IP address before you can enable remote logging.
`facility <daemon|local0|local1|local2|local3|local4|local5|local6|local7>`	Specifies remote logging facility.
`level <critical|informational|none|serious>`	Specifies the level of system messages to send to the remote system log server. • critical—only 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

Table continues…

Variable	Value
	• informational—only messages classified as informational are sent to the remote system log server • none—no system log messages are sent to the remote system log server

Disabling remote system logging using ACLI

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

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. To disable the remote system log, use the following command:

```
no logging remote [address] [secondary-address] [enable] [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.
`secondary-address`	Clears the secondary remote system log server IP address.
`enable`	Disables system message logging on the remote server.
`level`	Clears the remote server logging level.

Restoring remote system logging to default using ACLI

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

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. To disable the remote system log, use the following command:

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

Variable definitions

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

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

Chapter 5: 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

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 EAP - 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.

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 mode 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 mode 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 mode ID.
ModId	Indicates the ID of the mode.
Name	Indicates the name of the mode.

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

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

Variable Definitions

The following table describes the command parameters.

Variable	Value
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.

Viewing the stack-monitor

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

Procedure steps

1. Access the Privileged Exec mode.
2. Enter the following command:

```
show stack-monitor
```

Job Aid

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

```
4548GT-PWR#show stack-monitor
Status: disabled
Stack size: 2
Trap interval: 60
4548GT-PWR#
```

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 the default values.

Procedure Steps

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

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

Variable Definitions

The following table describes the command parameters.

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

Procedure steps

1. Access the 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. Access the Global Configuration mode.

2. Enter the following command:

   ```
   no stack monitor
   ```

Configure Stack Health Monitoring and Recovery

Use the following procedures to configure Stack Health Monitoring and Recovery.

Rebooting stack units on failure using ACLI

Use this procedure to reboot stack units when the system detects failure of stacking.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure Steps

1. To configure the system to reboot failed stacking units, enter the following command:

   ```
   stack reboot-on-failure
   ```

Displaying the status of stack reboot on failure using ACLI

Use this procedure to display the status of rebooting of stack units on failure.

Prerequisites

- Log on to the Privileged Exec mode in ACLI.

Note:

By default, stack reboot-on-failure is enabled on the switch.

Procedure Steps

1. To display the status of stack reboot-on-failure, enter the following command:

   ```
   show stack reboot-on-failure
   ```

Disabling stack reboot on failure

Use this procedure to disable stack reboot on failure.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure Steps

1. To disable `stack reboot on failure`, enter the following command:

   ```
   no stack reboot-on-failure
   ```

Configuring stack retry count using ACLI

Use this procedure to configure the number of times the system attempts to reach a unit before it indicates that the unit is down.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure Steps

1. To configure stack retry count, enter the following command:

```
Stack retry-count [retry-count]
```

Variable definitions

The following table describes the command parameter:

Variable	Value
retry count	Sets the retry count for the stack. The retry count is a value in a range from 0 to 4,294,967,295. Default value: 0 **Note:** To use the command, you must enter a value.

Displaying stack retry count using ACLI

Use this procedure to display the stack retry count value.

Prerequisites

- Log on to the Privileged Exec mode in ACLI.

Procedure Steps

1. To display the stack retry count, enter the following command:

```
show stack retry-count
```

Displaying stack health

Use this procedure to display stack health information.

Procedure Steps

1. Access the Privileged Exec mode.
2. Enter the following command:

```
show stack health
```

Job Aid

The following figure is an example of the show stack health command output when the stack is formed but the initialization process is not complete.

```
#show stack health
Switch Units Found = 8
Stack Health Check = OK - RESILIENT
Stack Diagnosis = Stack in full resilient mode.

--------------------------------------------------------------------------
UNIT#       Switch Model        Cascade Up      Cascade Down
--------------------------------------------------------------------------
1 (Base)     4526GTX                OK             OK
2            4526GTX-PWR            OK             OK
3            4524GT                 OK             OK
4            4526T                  OK             OK
5            4526T-PWR              OK             OK
6            4548GT-PWR             OK             OK
7            4550T                  OK             OK
8            4526FX                 OK             OK
```

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

```
#show stack health
Switch Units Found = 7
Stack Health Check = WARNING - NON-RESILIENT
Stack Diagnosis = Stack in non-resilient mode.
Recommend to add/replace the identified cable(s).

--------------------------------------------------------------------------
UNIT#       Switch Model        Cascade Up            Cascade Down
--------------------------------------------------------------------------
1 (Base)     4526GTX                OK                     OK
2            4526GTX-PWR            OK                     OK
3            4524GT                 OK                     OK
4            4526T                  OK           LINK DOWN or MISSING
6            4548GT-PWR      LINK DOWN or MISSING          OK
7            4550T                  OK                     OK
8            4526FX                 OK                     OK
```

The following figure 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.

```
Switch Units Found = 8
Stack Health Check = WARNING - NON-RESILIENT
Stack Diagnosis = Stack in non-resilient mode
Recommend to add/replace the identified cable(s).

--------------------------------------------------------------------------
UNIT#       Switch Model        Cascade Up      Cascade Down
--------------------------------------------------------------------------
1 (Base)     4526GTX                OK             OK
2            4526GTX-PWR            OK             OK
3            4524GT                 OK             OK
4            4526T                  OK             OK
5            4526T-PWR              OK             OK
6            4548GT-PWR             OK       UP WITH ERRORS
7            4550T            UP WITH ERRORS       OK
8            4526FX                 OK             OK
```

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

```
#show stack health
Switch Units Found = 8
Stack Health Check = OK - RESILIENT
Stack Diagnosis = Stack in full resilient mode.

--------------------------------------------------------------------------
UNIT#             Switch Model        Cascade Up    Cascade Down
--------------------------------------------------------------------------
1                 4526GTX                OK            OK
2 (Temporary Base) 4526GTX-PWR           OK            OK
3                 4524GT                 OK            OK
4                 4526T                  OK            OK
5                 4526T-PWR              OK            OK
6                 4548GT-PWR             OK            OK
7                 4550T                  OK            OK
8                 4526FX                 OK            OK
```

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.

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

1. To show stacking statistics, enter the following command:

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

Variable Definitions

The following table describes the command parameters.

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

Job aid

The following tables describe 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
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

1. To clear stacking statistics, enter the following command:

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

Variable Definitions

The following table describes the command parameters.

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

Using the stack loopback test

Use this procedure to complete a stack loopback test

Note:

Stack Reboot on Failure must be disabled before running this test. To disable rebooting of stack units on failure see Disabling stack reboot on failure on page 50

Procedure Steps

1. Access the Privileged Exec mode.
2. Enter the following command to carry out the internal loopback test for the stack ports:

   ```
   stack loopback-test internal
   ```

3. Enter the following command to carry out the external loopback test for the stack ports:

   ```
   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:

```
4524GT#stack loopback-test internal
Testing uplink port … ok


Testing downlink port … ok
Internal loopback test PASSED.
4524GT#
4524GT#stack loopback-test external
External loopback test PASSED.
4524GT#
```

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

```
4524GT#stack loopback-test internal
Testing uplink port … Failed
Testing downlink port … ok
Internal loopback test FAILED.
4524GT#
```

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:

```
4524GT#stack loopback-test external
External loopback test FAILED. Your stack cable might be damaged.
4524GT#
```

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

```
4548GT-PWR#stack loopback-test internal
Stack loopback test affects the functioning of the stack.
You should run this in stand-alone mode
4548GT-PWR#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.

Note:

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

Procedure Steps

1. Access the Privileged Exec mode.
2. Enter the following command:

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

   Tip:

   If you issue the command with no parameters, the system displays the port status for all ports.

Validating port operational status

Prerequisites

- Using ACI, configure the EAP status for some ports as unauthorized
- Configure VLACP on port 1 from a 4000 unit and on port 2 on another 4000 unit. Create a link between these 2 ports.

Procedure steps

1. To verify EAP port operational status, enter the following command:

   ```
   show interfaces
   ```

   The system displays the EAP status as Down for the unauthorized EAP ports
2. To verify VLACP port operational status, enter the following command:

   ```
   show interfaces
   ```

   The VLACP status is UP for the port where you entered the command.

   When you disconnect the link from the other switch, the system displays the VLACP status as Down.
3. To verify STP port operational status, after the switch boots, enter the following command:

   ```
   show interfaces
   ```

   The system displays STP Status as Listening.

   After a brief interval, the system displays the STP status as Learning.

   After the forward delay interval elapses, enter the following command:

   ```
   show interfaces
   ```

   The system displays the STP status as Forwarding.

Showing port information

You can display all of the configuration information for a specific port in one command.

The config keyword displays information specific to the port configuration.

Procedure steps

1. Access the Privileged Exec mode.
2. Enter the following command:

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

Job aid

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

Example

```
4526T#show interfaces 1/1-2 config

Unit/Port:  1/1
Trunk:
Admin:  Disable
Oper:  Down
Oper EAP:  Up
Oper VLACP:  Down
Oper STP:  Disabled
Link:  Down
LinkTrap:  Enabled
Autonegotiation:  Enabled

Unit/Port:  1/2
Trunk:
Admin:  Enable
Oper:  Down
Oper EAP:  Up
Oper VLACP:  Down
Oper STP:  Forwarding
Link:  Down
LinkTrap:  Enabled
Autonegotiation:  Enabled
```

Table 3: VLAN interfaces configuration

Unit/Port	Filter Untagged Frames	Filter Unregistered Frames	PVID	PRI	Tagging	Name
1/1	No	Yes	256	0	UntagAll	Unit 1, Port 1
1/2	No	Yes	2	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	256	VLAN #256				
1/2	2	VLAN-2				

Table 5: Spanning-tree port configurations

Unit	Port	Trunk	Participation	Priority	Path	Cost	State
1	1		Disabled				
1	2		Normal	Learning	128	20000	Forwarding

Viewing Environmental status using ACLI

Perform this procedure to view the Environmental status of the switch or stack.

Procedure steps

1. Access the User EXEC mode.
2. To view the Environmental status of the switch, enter the following command:

   ```
   show environmental
   ```

Job aid

The following figure shows sample output for the **`show environmental`** command.

```
4524GT-PWR>show environmental
Unit# PSU1      PSU2      FAN1 FAN2 FAN3 FAN4 Temperature
----- --------- --------- ---- ---- ---- ---- -----------
1     Primary   N/A       OK   OK   OK   OK   30C

Unit# Model        Switch Capacity Saving PoE Saving
----- ------------ ---------------------- --------------------
1     4524GT-PWR   0.0 watts              0.0 watts
-------------------------------------------------------------
TOTAL              0.0 watts              0.0 watts
=============================================================
4524GT-PWR>
```

Displaying Many-to-Many port-mirroring using ACLI

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

Prerequisites

- Use this command in the Privileged Executive mode.

Procedure steps

Procedure steps

1. Enter the following command:

   ```
   show port-mirroring
   ```

Configuring Many-to-Many port-mirroring using ACLI

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

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

1. Enter the following command:

   ```
   port-mirroring <1-4> [allow-traffic] mode {disable |Adst monitor-
   port <portList> mirror-MAC-A <H.H.H>|Asrc monitor-port <portList>
   mirror-MAC-A <H.H.H> mirror-MAC-B <H.H.H> | AsrcBdstOrBsrcAdst
   monitor-port <portList> mirror-MAC-A <H.H.H> mirror-MAC-B <H.H.H> |
   AsrcOrAdst monitor-port <portList> mirror-MAC-A <H.H.H> |ManyToOneRx
   ```

```
monitor-port <portList> mirror-ports <portList> |ManyToOneRxTx
monitor-port <portList> mirror-ports <portList> |ManyToOneTx
monitor-port <portList> mirror-ports <portList> |Xrx 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>> |
XrxYtx monitor-port <portList> mirror-port-X <portList> mirror-port-
Y <portList> |XrxYtxOrYrxXtx monitor-port <portList> mirror-port-X
<portList> mirror-port-Y <portList> |Xtx monitor-port <portList>
mirror-port-X <portList> [rspan-vlan <VID>]
```

Example

Enable port-mirroring for first instance

```
# port-mirroring mode Xrx monitor-port 10 mirror-port-X
17
```

Example

Enable port-mirroring for instance 3

```
#port-mirroring 3 mode Asrc monitor-port 19 mirror-mac-a
00:00:aa:bb:cc:dd
```

Variable definitions

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

Variable	Value
<1-4>	Port-mirroring instance number. Default is 1.
allow-traffic	Enables bi-direction Monitor Port. **Note:** You cannot use this parameter to configure RSPAN sessions, because the local monitoring port allows traffic by default during an RSPAN session. If the **allow-traffic** parameter is used with the **rspan-vlan <VID>** parameter, an error message is displayed.
Adst	Mirror packets with destination MAC address A.
Asrc	Mirror packets with source MAC address A.
AsrcBdst	Mirror packet 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.

Table continues…

Variable	Value
AsrcOrAdst	Mirror packet with source or destination MAC address A.
ManyToOneRx	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 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.
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 .
rspan-vlan <VID>	Enables remote port-mirroring and specifies the VLAN for mirrored traffic.

Disabling many-to-many port-mirroring

Use this procedure to disable many-to-many port-mirroring

Prerequisites

- Use this command in the Global Configuration mode.

Procedure steps

1. Enter one of the following commands to disable a specific instance:

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

   OR

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

2. Enter the following command to disable all instances:

   ```
   no port-mirroring
   ```

Example

Disable port-mirroring for instance 3

```
#no port-mirroring 3
```

Example

Disable all port-mirroring instances

```
#no port-mirroring
```

Variable definitions

The following table describes the parameters for the **no port-mirroring** command.

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

Configuring an RSPAN source session

Use this procedure to configure an RSPAN source session.

Before you begin

Create an RSPAN VLAN and establish port membership.

About this task

An RSPAN source session associates a port mirroring instance with an RSPAN VLAN. The output of this session is a stream of packets sent to the RSPAN VLAN.

Procedure

1. Enter Global Configuration mode

   ```
   enable

   configure terminal
   ```

2. Use the following command to configure the RSPAN source session:

   ```
   port-mirroring [<1-4>] mode {disable | Adst monitor-port <portList>
   mirror-MAC-A <H.H.H> | Asrc monitor-port <portList> mirror-MAC-A
   <H.H.H> | AsrcBdst monitor-port <portList> mirror-MAC-A <H.H.H>
   mirror-MAC-B <H.H.H> | AsrcBdstOrBsrcAdst monitor-port <portList>
   mirror-MAC-A <H.H.H> mirror-MAC-B <H.H.H> | AsrcOrAdst monitor-port
   <portList> mirror-MAC-A <H.H.H> | ManyToOneRx monitor-port
   <portList> mirror-ports <portList> | ManyToOneRxTx monitor-port
   <portList> mirror-ports <portList> | ManyToOneTx monitor-port
   <portList> mirror-ports <portList> | Xrx 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> | XrxYtx monitor-port <portList>
   mirror-port-X <portList> mirror-port-Y <portList> | XrxYtxOrYrxXtx
   monitor-port <portList> mirror-port-X <portList> mirror-port-Y
   ```

```
<portList> | Xtx monitor-port <portList> mirror-port-X <portList>
rspan-vlan <VID>
```

3. Use the following command to display and verify the RSPAN settings:

```
show port-mirroring
```

Example

The following example displays sample output for configuring an RSPAN source session:

```
ERS4000> enable
ERS4000# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ERS4000(config)# vlan create 1009 type port remote-span
ERS4000(config)# vlan members add 1009 1/26
ERS4000(config)# port-mirroring 2 ManyToOneRx monitor-port 1/26 mirror-ports 1/1-1/12
rspan-vlan 1009
ERS4000(config)# show port-mirroring
```

Variable definitions

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

Variable	Value
<1-4>	Port-mirroring instance number. Default is 1.
allow-traffic	Enables bi-direction Monitor Port.
Adst	Mirror packets with destination MAC address A.
Asrc	Mirror packets with source MAC address A.
AsrcBdst	Mirror packet 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 packet with source or destination MAC address A.
ManyToOneRx	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 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.

Table continues…

Variable	Value
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 .
rspan-vlan <VID>	Enables remote port-mirroring and specifies the VLAN for mirrored traffic.

Configuring an RSPAN destination session

Use this procedure to configure an RSPAN destination session.

Before you begin

Create an RSPAN VLAN.

About this task

An RSPAN destination session associates the destination port with an RSPAN VLAN. The destination session collects all RSPAN VLAN traffic and sends it out the designated RSPAN destination port.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Use the following command to configure an RSPAN destination session:

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

Example

The following example displays sample output for configuring an RSPAN destination session:

```
ERS4000> enable
ERS4000# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ERS4000(config)# vlan create 1009 type port remote-span
ERS4000(config)# vlan members add 1009 1/2,26
ERS4000(config)# port-mirroring rspan 2 destination-port 1/26 vlan 1009
ERS4000(config)#show port-mirroring rspan
```

Variable definitions

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

Variable	Value
[no]	Disables the destination RSPAN session.
<1-4>	RSPAN destination session number. Default is 1.
[destination-port <port>]	Specifies the port to be used as the destination port.
[vlan <VID>]	Specifies the RSPAN VLAN to be associated with the destination port.

Displaying RSPAN information

Use this procedure to display RSPAN information.

Procedure

1. Enter Privileged EXEC mode.
2. Use the following command to display RSPAN information:

   ```
   show port-mirroring rspan
   ```

Chapter 6: RMON configuration using the ACLI

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

Viewing the RMON alarms

Use this procedure to display information about RMON alarms.

Procedure steps

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

```
show rmon alarm
```

Viewing the RMON events

Use this procedure to display information regarding RMON events.

Procedure steps

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

```
show rmon event
```

Viewing the RMON history

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

Procedure steps

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

```
show rmon history
```

Viewing the RMON statistics

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

Procedure steps

1. Access the Global Configuration mode
2. Enter the following command;

```
show rmon stats
```

Configuring RMON alarms

Use this procedure to set RMON alarms and thresholds.

Procedure steps

1. Access the Global Configuration mode.
2. At the command prompt, enter the following command:

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

Variable Definitions

The following table describes the command parameters.

Variable	Value
<1-65535>	Unique index for the alarm entry.
<WORD>	The MIB object to be monitored. This is an object identifier, and for most available objects. You can use 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 when the rising threshold is crossed. If omitted, or if an invalid event entry is referenced, no event is triggered. Unique index for the alarm entry.
falling-threshold <-2147483648-2147483647 > [<1-65535>]	The first integer value is the falling threshold value. The optional second integer specifies the event entry to be triggered when the falling threshold is crossed. If omitted, or if an invalid event entry is referenced, no event is triggered. Unique index for the alarm entry.
[owner <LINE>]	Specify an owner string to identify the alarm entry.

Deleting RMON alarms

Use this procedure to delete RMON alarm table entries.

Tip:

When you omit the variables, the system clears all entries in the table.

Procedure steps

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

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

Variable Definitions

The following table describes the command parameters.

Variable	Value
1-65535	Unique index for the event entry.

Configuring RMON events settings

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

Procedure steps

1. Access the 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.

Variable	Value
<1-65535>	Unique index for the event entry.
[log]	Records events in the log table.
[trap]	Generates SNMP trap messages for events.
[description <LINE>]	Specifies a textual description for the event.
[owner <LINE>]	Specifies an owner string to identify the event entry.

Deleting RMON events settings

Use this procedure to delete RMON event table entries.

Tip:

When you omit the variable, the system clears all entries in the table.

Procedure steps

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

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

Variable Definitions

The following table describes the command parameters.

Variable	Value
1-65535	Unique index for the event entry.

Configuring RMON history settings

Use this procedure to configure RMON history settings.

Procedure steps

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

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

Variable Definitions

The following table describes the command parameters.

Variable	Value
<1-65535>	Unique index for the history entry.
<LINE>	Specifies 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>]	Specifies an owner string to identify the history entry.

Deleting RMON history settings

Use this procedure to delete RMON history table entries. When you omit the variable, all entries in the table are cleared.

Procedure steps

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

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

Variable Definitions

The following table describes the command parameters.

Variable	Value
1-65535	Unique index for the event entry.

Configuring RMON statistics settings

Use this procedure to configure RMON statistics settings.

Procedure steps

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

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

Variable Definitions

The following table describes the command parameters.

Variable	Value
<1-65535>	Unique index for the stats entry.
[owner <*LINE*>]	Specifies an owner string to identify the stats entry.

Deleting RMON statistics settings

Use this procedure to turn off RMON statistics.

Tip:

When omit the variable, the system clears all entries in the table.

Procedure steps

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

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

Variable Definitions

The following table describes the command parameters.

Variable	Value
1-65535	Unique index for the event entry.

Chapter 7: IPFIX configuration using ACLI

This chapter describes the procedures you can use to configure IP Flow Information Export (IPFIX) using Avaya Command Line Interface (ACLI).

Global IPFIX management using ACLI

Use the information in this section to enable or disable IPFIX globally on a switch or stack.

Enabling IPFIX globally using ACLI

Use this procedure to enable IPFIX globally for a switch or stack.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enter the following command:

```
ip ipfix enable
```

Disabling IPFIX globally using ACLI

Use this procedure to disable IPFIX globally for a switch or stack.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enter any one of the following commands:

```
no ip ipfix enable
```

```
default ip ipfix enable
```

Viewing the global IPFIX status using ACLI

Use this procedure to display the global IPFIX operational status for a switch or stack.

Prerequisites

- Log on to the Privileged EXEC mode in ACLI.

Procedure steps

Enter the following command:

```
show ip ipfix
```

IPFIX flow management using ACLI

Use the information in this section to configure and manage IPFIX flow for a standalone switch or a switch in a stack.

Configuring the IPFIX aging interval using ACLI

Use this procedure to configure the IPFIX flow record aging interval for a standalone switch or a switch in a stack.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enter the following command:

```
ip ipfix slot <unit_number> aging-interval <0-2147400>
```

Variable definitions

The following table defines optional parameters that you enter after the **`ip ipfix slot <unit_number> aging-interval <0-2147400>`** command.

Variable	Value
`aging-interval <0-2147400>`	Specifies the aging interval of the flow record in seconds. Values range from 0–2147400 seconds. Aging time is the period of time in which all records are verified if they are updated. If no new updates

Table continues…

Variable	Value
	are found between two checks, the system deletes the records.
`slot <unit_number>`	Specifies whether the switch is a standalone or part of a stack. A value of 1 indicates a standalone switch.

Changing the IPFIX aging interval to default using ACLI

Use this procedure to change the IPFIX flow record aging interval to the default value of 30 seconds for a standalone switch or a switch in a stack.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enter the following command:

```
default ip ipfix slot <unit_number> aging-interval
```

Enabling the IPFIX exporter using ACLI

Use this procedure to enable the IPFIX exporter for a standalone switch or a switch stack.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enter any one of the following commands:

- `ip ipfix exporter-enable`
- `default ip ipfix exporter-enable`

Disabling the IPFIX exporter using ACLI

Use this procedure to disable the IPFIX exporter for a standalone switch or a switch stack.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enter the following command:

```
no ip ipfix exporter-enable
```

Configuring the IPFIX export interval using ACLI

Use this procedure to configure the IPFIX export interval for a standalone switch or a switch stack.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enter the following command:

```
ip ipfix export-interval <10-3600>
```

Variable definitions

The following table defines parameters that you enter with the **`ip ipfix export-interval <10-3600>`** command.

Variable	Value
`export-interval <10-3600>`	Specifies the frequency of data exports to the collector in seconds. Values range from 10 to 3600 seconds. The default is 50 seconds.

Changing the IPFIX export interval to default using ACLI

Use this procedure to change the IPFIX export interval for a standalone switch or a switch stack to the default value of 50 seconds.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enter the following command:

```
default ip ipfix export-interval
```

Configuring the IPFIX refresh interval template using ACLI

Use this procedure to configure the IPFIX refresh interval template for a standalone switch or a switch stack.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enter the following command:

```
ip ipfix template-refresh-interval <300-3600>
```

Variable definitions

The following table defines parameters that you enter with the **`ip ipfix template-refresh-interval <300-3600>`** command.

Variable	Value
`template-refresh-interval <300-3600>`	Specifies the refresh timeout interval template in seconds. Values range from 300 to 3600. The default is 1800 seconds. The template is sent out to the collector either at the configured interval or after the specified template packets refresh number is reached, whichever occurs first. The template is also sent out to the collector when globally enabling IPFIX.

Changing the IPFIX refresh interval template to default using ACLI

Use this procedure to change the IPFIX refresh interval template for a standalone switch or a switch stack to the default value of 1800 seconds.

The template is sent out to the collector either at the configured interval or after the specified template packets refresh number is reached, whichever occurs first.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enter the following command:

```
default ip ipfix template-refresh-interval
```

Configuring the IPFIX refresh packets template using ACLI

Use this procedure to configure the IPFIX refresh packets template for a standalone switch or a switch stack.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

Enter the following command:

```
ip ipfix template-refresh-packets <10000-100000>
```

Variable definitions

The following table defines parameters that you enter with the **`ip ipfix template-refresh-packets <10000-100000>`** command.

Variable	Value
`template-refresh-packets <10000-100000>`	Specifies the refresh packets template limit in numbers of packets. Values range from 10000 to 100000 packets. The default is 10000 packets. The template is sent out to the collector either after the configured template packets refresh number is reached or at the specified refresh interval, whichever occurs first. The template is also sent out to the collector when globally enabling IPFIX.

Changing the IPFIX refresh packets template to default using ACLI

Use this procedure to change the IPFIX refresh packets template for a standalone switch or a switch stack to the default value of 10000 packets.

Prerequisites

- Log on to the Global Configuration mode in ACLI.

Procedure steps

1. To change the IPFIX refresh packets template to default, enter the following command:

   ```
   default ip ipfix template-refresh-packets
   ```

Viewing IPFIX flow information using ACLI

Use this procedure to display configured IPFIX flow information.

Prerequisites

- Log on to the User EXEC mode in ACLI.

Procedure steps

1. To view IPFIX flow information, enter the following command:

   ```
   show ip ipfix slot <unit_number>
   ```

Variable definitions

The following table defines parameters that you enter with the **`show ip ipfix slot <unit_number>`** command.

Variable	Value
`slot <unit_number>`	Displays information for a switch that is a standalone or part of a stack. A value of 1 indicates a standalone switch.

Job aid: IPFIX flow information display

The following table provides information to help you understand information displayed with the **`show ip ipfix slot <unit_number>`** command.

Variable	Value
Aging Interval (sec)	Indicates the aging interval of the flow record in seconds. Values range from 0–2147400 seconds. The default is 30 seconds.
Active Timeout (min)	Indicates the flow record active timeout value in minutes. This is not a configurable value.
Export Interval (sec)	Indicates the frequency of data exports to the collector in seconds. Values range from 10 to 3600 seconds. The default is 50 seconds.
ExportState	Indicates the operational state of the exporter. The default is enabled.
Template Refresh (sec)	Indicates the template refresh timeout in seconds. Values range from 300 to 3600. The default is 1800 seconds. The template is sent out to the collector either at the configured interval or after the specified template

Table continues…

Variable	Value
	packets refresh number is reached, whichever occurs first.
Template Refresh (pkts)	Indicates the template refresh timeout in numbers of packets. Values range from 10000 and 100000 packets. The default is 10000 packets. The template is sent out to the collector either after the configured template packets refresh number is reached or at the specified refresh interval, whichever occurs first.

IPFIX collector management using ACLI

Use the information in this section to enable or disable IPFIX collectors, and to display configured IPFIX collector configuration information.

Enabling an IPFIX collector using ACLI

Use this procedure to enable an IPFIX collector for a standalone switch or a switch stack.

Prerequisites

- Log in to the Global Configuration mode in ACLI

Procedure steps

1. To enable an IPFIX collector, enter one of the following commands:
   - `ip ipfix collector <A.B.C.D> enable`
   - `default ip ipfix collector <A.B.C.D> enable`

Variable definitions

The following table defines parameters that you enter with the **`ip ipfix collector <A.B.C.D> enable`** or the **`default ip ipfix collector <A.B.C.D> enable`** command.

Variable	Value
`<A.B.C.D>`	Specifies the IPFIX collector IP address.

Disabling an IPFIX collector using ACLI

Use this procedure to disable an IPFIX collector for a standalone switch or a switch stack.

Prerequisites

- Log in to the Global Configuration mode in ACLI

Procedure steps

1. To disable an IPFIX collector, enter the following command:

   ```
   no ip ipfix collector <A.B.C.D> enable
   ```

Variable definitions

The following table defines parameters that you enter with the **`no ip ipfix collector <A.B.C.D> enable`** command.

Variable	Value
`<A.B.C.D>`	Specifies the IPFIX collector IP address.

Viewing the IPFIX collector information using ACLI

Use this procedure to display IPFIX collector configuration information for a standalone switch or a switch stack.

Procedure steps

1. To view information for all configured IPFIX collectors enter the following command:

   ```
   show ip ipfix collector
   ```

2. To view information for a specific configured IPFIX collector, enter the following command:

   ```
   show ip ipfix collector <A.B.C.D>
   ```

Variable definitions

The following table defines parameters that you enter with the **`show ip ipfix collector <A.B.C.D>`** command.

Variable	Value
`<A.B.C.D>`	Displays the operational status for a specific IPFIX collector IP address.

Port IPFIX management using ACLI

Use the information in this section to enable or disable IPFIX for one or more switch ports on a standalone switch or a switch that is part of a stack.

Enabling port-based IPFIX for a standalone switch using ACLI

Use this procedure to enable IPFIX for one or more ports on a standalone switch.

Prerequisites

- Log in to the Interface Configuration mode in ACLI

Procedure steps

1. To enable IPFIX for the selected port or ports, enter the following command:

   ```
   ip ipfix enable
   ```

2. To enable IPFIX for alternate ports, enter the following command:

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

Variable definitions

The following table defines parameters that you enter with the **`ip ipfix port <port_list> enable`** command.

Variable	Value
`port <port_list>`	Specifies an individual port or list of ports.

Disabling port-based IPFIX for a standalone switch using ACLI

Use this procedure to disable IPFIX for one or more ports on a standalone switch.

Prerequisites

- Log in to the Interface Configuration mode in ACLI

Procedure steps

1. To disable IPFIX for the selected port or ports, enter the following command:

   ```
   no ip ipfix [enable] [port <port_list> enable]
   ```

Variable definitions

The following table defines optional parameters that you can enter with the **`no ip ipfix [enable] [port <port_list> enable]`** command.

Variable	Value
`enable`	Disables IPFIX for the selected port or ports.
`port <port_list> enable`	Disables IPFIX for an alternate individual port or list of ports.

Changing port-based IPFIX for a standalone switch to default using ACLI

Use this procedure to change the IPFIX operational status to default for one or more ports on a standalone switch.

Prerequisites

- Log in to the Interface Configuration mode in ACLI

Procedure steps

1. To change the IPFIX operational status for one or more ports, enter the following command:

   ```
   default ip ipfix [enable] [port <port_list> enable]
   ```

2. To enable IPFIX for alternate ports, enter the following command:

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

Variable definitions

The following table defines optional parameters that you can enter with the **`default ip ipfix [enable] [port <port_list> enable]`** command.

Variable	Value
`enable`	Changes the IPFIX operational status for the selected port or ports to default.
`port <port_list> enable`	Changes the IPFIX operational status for a port or list of ports to default.

Viewing the port-based IPFIX status for a standalone switch using ACLI

Use this procedure to display the IPFIX operational status for one or more ports on a standalone switch.

Prerequisites

- Log in to the User Exec mode in ACLI

Procedure steps

1. To display the IPFIX operational status for all switch ports, enter the following command:

   ```
   show ip ipfix interface
   ```

2. To display the IPFIX operational status for specific switch ports, enter the following command:

   ```
   show ip ipfix interface <port_list>
   ```

Variable definitions

The following table defines parameters that you enter with the **show ip ipfix interface <port_list>** command.

Variable	Value
<port_list>	Specifies a specific port or list of ports for which to display the IPFIX operational mode for to default.

Enabling port-based IPFIX for a stack switch using ACLI

Use this procedure to enable IPFIX for one or more ports on a switch that is part of a stack.

Prerequisites

- Log in to the Interface Configuration mode in ACLI

Procedure steps

1. To enable IPFIX for the selected port or ports, enter the following command:

   ```
   ip ipfix enable
   ```

2. To enable IPFIX for alternate ports, enter the following command:

   ```
   ip ipfix port <unit_number/port_list> enable
   ```

Variable definitions

The following table defines parameters that you enter with the **ip ipfix port <unit_number/port_list> enable** command.

Variable	Value
port <unit_number/port_list>	Specifies switch number in the stack and an individual port or list of ports.

Disabling port-based IPFIX for a stack switch using ACLI

Use this procedure to disable IPFIX for one or more ports on a switch that is part of a stack.

Prerequisites

- Log in to the Interface Configuration mode in ACLI

Procedure steps

1. To disable IPFIX for the selected port or ports, enter the following command:

   ```
   no ip ipfix enable
   ```

2. To disable IPFIX for alternate ports, enter the following command:

```
no ip ipfix port <unit_number/port_list> enable
```

Variable definitions

The following table defines parameters that you enter with the **ip ipfix port <unit_number/port_list> enable** command.

Variable	Value
port <unit_number/port_list>	Specifies a switch number in the stack and an individual port or list of ports.

Changing port-based IPFIX for a stack switch to default using ACLI

Use this procedure to change the IPFIX operational status to default for one or more ports on a switch that is part of a stack.

Prerequisites

- Log in to the Interface Configuration mode in ACLI

Procedure steps

1. To change the IPFIX operational status for the selected port or ports, enter the following command:

   ```
   default ip ipfix enable
   ```

2. To change the IPFIX operational status for alternate port or ports, enter the following command:

   ```
   default ip ipfix port <unit_number/port_list> enable
   ```

Variable definitions

The following table defines parameters that you enter with the **default ip ipfix port <unit_number/port_list> enable** command.

Variable	Value
port <unit_number/port_list>	Specifies a switch number in the stack and an individual port or list of ports.

Viewing the port-based IPFIX status for a stack switch using ACLI

Use this procedure to display the IPFIX operational status for one or more ports on a standalone switch.

Prerequisites

- Log in to the User Exec mode

Procedure steps

1. To display the IPFIX operational status for all ports in the stack, enter the following command:

   ```
   show ip ipfix interface
   ```

2. To display the IPFIX operational status for specific ports in the stack, enter the following command:

   ```
   show ip ipfix interface <unit_number/port_list>
   ```

Variable definitions

The following table defines parameters that you enter with the **`show ip ipfix interface <unit_number/port_list>`** command.

Variable	Value
`<unit_number/port_list>`	Specifies a switch number in the stack and an individual port or list of ports.

Viewing the IPFIX table using ACLI

Use this procedure to sort and display IPFIX statistics for a standalone switch or a switch stack.

Prerequisites

- Log in to the User Exec mode.

Procedure steps

1. To view the IPFIX table, enter the following command:

   ```
   show ip ipfix table <unit_number> [sort-by <sort_rule>] [sort-order
   <sort_order>] [display <num_entries>]
   ```

Variable definitions

Variable	Value
`display <num_entries>`	Specifies the number of entries to display. Values include: • all—displays all available entries • top-10—displays first 10 entries • top-25—displays first 25 entries

Table continues…

Variable	Value
	• top-50—displays first 50 entries • top-100—displays first 100 entries • top-200—displays first 200 entries
`sort-by <sort_rule>`	Specifies a rule to sort data by. Values include: • byte-count—data byte number • dest-addr—destination IP address • first-pkt-time—first packet time • last-pkt-time—last packet time • pkt-count—packet number
	• port—port number • protocol—protocol number • source-addr—source IP address • TCP-UDP-dest-port—TCP/UDP destination port • TCP-UDP-src-port—TCP/UDP source port • TOS—type of service
`sort-order <sort_order>`	Specifies the order in which to sort data. Values include: • ascending • descending
`<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.

Chapter 8: SLA Monitor Configuration using ACLI

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

Related Links

Displaying SLA Monitor agent settings on page 89
Configuring the SLA Monitor on page 90

Displaying SLA Monitor agent settings

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

Procedure

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

   ```
   show application slamon agent
   ```

Example

```
4526T-PWR+>enable
4526T-PWR+#show application slamon agent

SLAMon Operational Mode: Disabled
SLAMon Agent Encryption: Supported
SLAMon Agent Address: 0.0.0.0
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: Disabled
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
```

Related Links

SLA Monitor Configuration using ACLI on page 89

Configuring the SLA Monitor

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. Log on to Application Configuration mode in ACLI.
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>
   ```

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:

    The CLI commands from step 10 to 14 affect only the SLA Monitor (SLM) CLI commands and not the standard platform CLI commands.

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

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

    OR

    ```
    default slamon cli
    ```

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

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

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

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

    OR

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

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

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

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 [enable]
    ```

20. To disable the agent refuse server test mode, enter the following command:

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

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

```
4850GTS-PWR+>enable
4850GTS-PWR+#configure terminal
4850GTS-PWR+(config)#application
4850GTS-PWR+(config-app)#slamon oper-mode enable
4850GTS-PWR+(config-app)#show application slamon agent

SLAMon Operational Mode: Enabled
SLAMon Agent Encryption: Not Supported
SLAMon Agent Address: 172.16.120.20
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: Disabled
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
```

Next steps

If you have configured SLA Monitor yet the agent is not functioning 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.

If the agent is still not functioning, reset the system to ensure that the agent has started.

Variable definitions

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

Variable	Value
agent	Configures the SLA Monitor agent.
agent-comm-port <*0, 1024-65535*>	Configures the SLA Monitor agent-to-agent communication UDP port.
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	Configures the SLA Monitor agent CLI interface.
cli-timeout <*60–600*>	Configures the CLI timeout value in seconds. The default is 60 seconds. **Note:** The CLI commands only impact the SLA Monitor CLI and not the standard platform CLI.
ntr	Initiates the SLA Monitor NTR test.
oper-mode	You can enable or disable the SLA Monitor agent. By default, SLA Monitor agent 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.
rtp	Initiates the SLA Monitor RTP test.

Table continues…

Variable	Value
refuse-server-tests	Agent accepts 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	Configures the SLA Monitor server.
server-bypass	You can enable or disable the SLA Monitor agent server-bypass mode. 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.

Executing NTR test using ACLI

Use this procedure to execute a new trace route (NTR) test on the network to establish the 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 in ACLI.
2. To execute the NTR test, enter the following command:

   ```
   slamon ntr {A.B.C.D} <0-63>
   ```

Example

```
4850GTS-PWR+>enable
4850GTS-PWR+#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
4850GTS-PWR+(config)#application
4850GTS-PWR+(config-app)#slamon oper-mode enable
4850GTS-PWR+(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
4850GTS-PWR+(config-app)#
```

Variable definitions

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

Variable	Value
IPv4 Address *<A.B.C.D>*	Specifies the destination IP address. If no IP address is specified, the test execution fails.
DSCP *<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. The default value is 2.
period *<1000–200000>*	Specifies the interval between packets in microseconds, generated by the NTR test. The default interval is 20000 microseconds.

Executing RTP test using ACLI

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

Before you begin

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

Note:

You must enable the SLA Monitor agent ServerBypass mode for the RTP test to complete successfully.

Procedure

1. Enter Application Configuration mode in ACLI.
2. To execute the RPT test, enter the following command::

   ```
   slamon RTP {A.B.C.D} <0-63>
   ```

Example

```
4850GTS-PWR+>enable
4850GTS-PWR+#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
4850GTS-PWR+(config)#application
4850GTS-PWR+(config-app)#slamon oper-mode enable
4850GTS-PWR+(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
4850GTS-PWR+(config-app)#
```

Variable definitions

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

Variable	Value
IPv4 Address *<A.B.C.D>*	Specifies the destination IP address. If no IP address is specified, the test execution fails.
DSCP *<0–63>*	Specifies the DSCP value for use in packets that are generated by the RTP test.
npack *<10–100>*	Specifies the RTP npack value. The default value is 50.
nsync *<10–100>*	Specifies the RTP nsync value. The default value is 10.
period *<1000–200000>*	Specifies the interval between packets in microseconds, generated by the RTP test. The default interval is 20000 microseconds.

Chapter 9: 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).

Prerequisites

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

Port Mirroring using EDM

The following sections describe Port Mirroring:

- Viewing Port Mirroring using EDM
- Configuring Port Mirroring using EDM

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

The following table describes the Port Mirrors tab fields.

Variable	Value
Instance	Specifies the numerical assignment of the port mirroring (1-4)
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.
RspanVlan	Specifies the RspanVlan to be associated with a source port-mirroring instance.

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

Variable definitions

The following table describes the Port Mirrors tab fields.

Variable	Value
Instance	Indicates the Port Mirroring instance number (1-4)
Port Mode	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

Table continues…

Variable	Value
	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. • Xtx—Mirror packets transmitted on port X. The default value is Disabled.
Monitor Port	Specifies the monitoring 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 mirroring traffic is enabled.
RspanVlan	Specifies the RspanVlan to be associated with a source port-mirroring instance.

Remote Port Mirroring using EDM

Remote Switch Port ANalyzer (RSPAN), also known as Remote Port Mirroring, enhances port mirroring by enabling mirroring traffic to be sent to one or more switches or stacks on the network using an intermediate VLAN for forwarding the mirrored traffic.

Use the following procedures to configure source and destination sessions.

Configuring an RSPAN source session using EDM

Use the following procedure to configure an RSPAN source session..

Before you begin

Create a VLAN for RSPAN traffic and enable RSPAN on this VLAN.

About this task

An RSPAN source session associates a port mirroring instance with an RSPAN VLAN. The output of this session is a stream of packets sent to 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, double-click **Port Mirrors**.
4. On the toolbar, click **Insert**.

   The Insert Port Mirrors dialog box appears.
5. Configure the parameters as required.
6. In the **RspanVlan**field, select the VLAN for RSPAN traffic.
7. Click **Insert**.

Variable definitions

The following table describes the fields associated with the Port Mirrors tab.

Variable	Value
Instance	Numerical assignment of the port mirroring.
Port Mode	The port monitoring mode. The following options are available: • Adst • Asrc • AsrcBdst • AsrcBdstorBsrcAdst • AsrcorAdst • manytoOneRx • manytoOneRxTx • manytoOneTx • Xrx • XrxorXtx • XrxorYtx • XrxYtx • XrxYtxOrYrxXtx • Xtx The default value is Adst.
Monitor Port	The port that is the monitoring port.
PortListX	Ports monitored for XrX/Xtx, and manytoOne related mode.
PortListY	Ports monitored for Yrx/Ytx related mode.

Table continues…

Variable	Value
MacAddressA	MAC address of the monitored port using Sarc/Adst related mode.
MacAddressB	MAC address of the monitored portusing Bsrc/Bdst related mode.
Allow traffic	Allows or disallow traffic. **Note:** You cannot use the **Allow traffic** option with RSPAN.
RspanVlan	Specifies the RSPAN VLAN to be associated with a source port-mirroring instance.

Configuring an RSPAN destination session using EDM

Use the following procedure to configure an RSPAN destination session using EDM.

Before you begin

Create a VLAN for RSPAN traffic and enable RSPAN on this VLAN.

About this task

An RSPAN destination session associates the destination port with the RSPAN VLAN. The destination session collects all RSPAN VLAN traffic and sends it out the designated RSPAN destination port.

Procedure

1. From the navigation tree, click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **RSPAN**.
4. On the toolbar, click **Insert**.

   EDM displays the Insert RSPAN window.
5. Configure the parameters as required.
6. Click **Insert**.

Variable definitions

The following table describes the fields associated with the RSPAN tab.

Variable	Value
Instance	Specifies the destination session instance number.
DestinationPort	Specifies the port to be used as a destination port
RspanVlan	Specifies the RSPAN VLAN to be associated with the destination port.

Configuring Stack Monitor using EDM

Use the following procedure to configure the Stack Monitor.

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 **Stack Monitor** tab.
5. Select **StackErrorNotificationEnabled** to enable stack monitoring.
6. Set the stack size you want to monitor in the **ExpectedStackSize** field.
7. Sets the traps interval in the **StackErrorNotificationInterval** field.
8. Select **StackRebootUnitOnFailure** to enable rebooting of stack units on failure.
9. Set the retry count for the stack in the **StackRetryCount** field.
10. On the toolbar, click **Apply**.

Variable definitions

The following table describes the Stack Monitor tab fields.

Variable	Value
StackErrorNotificationEnabled	Enables or disables the Stack Monitoring feature.
ExpectedStackSize	Sets the size of the stack to monitor. Valid range is 2–8.
StackErrorNotificationInterval	Sets the interval between traps, in seconds. Valid range is 30 to 300 seconds.
StackRebootUnitOnFailure	Enables or disables the rebooting stack units on failure.
StackRetryCount	Sets the retry count for the stack. Valid range is 0-4294967295.

Job Aid

Figure 1 Stack monitor configuration using EDM on page 103 shows an example for configuring the stack monitor using EDM:

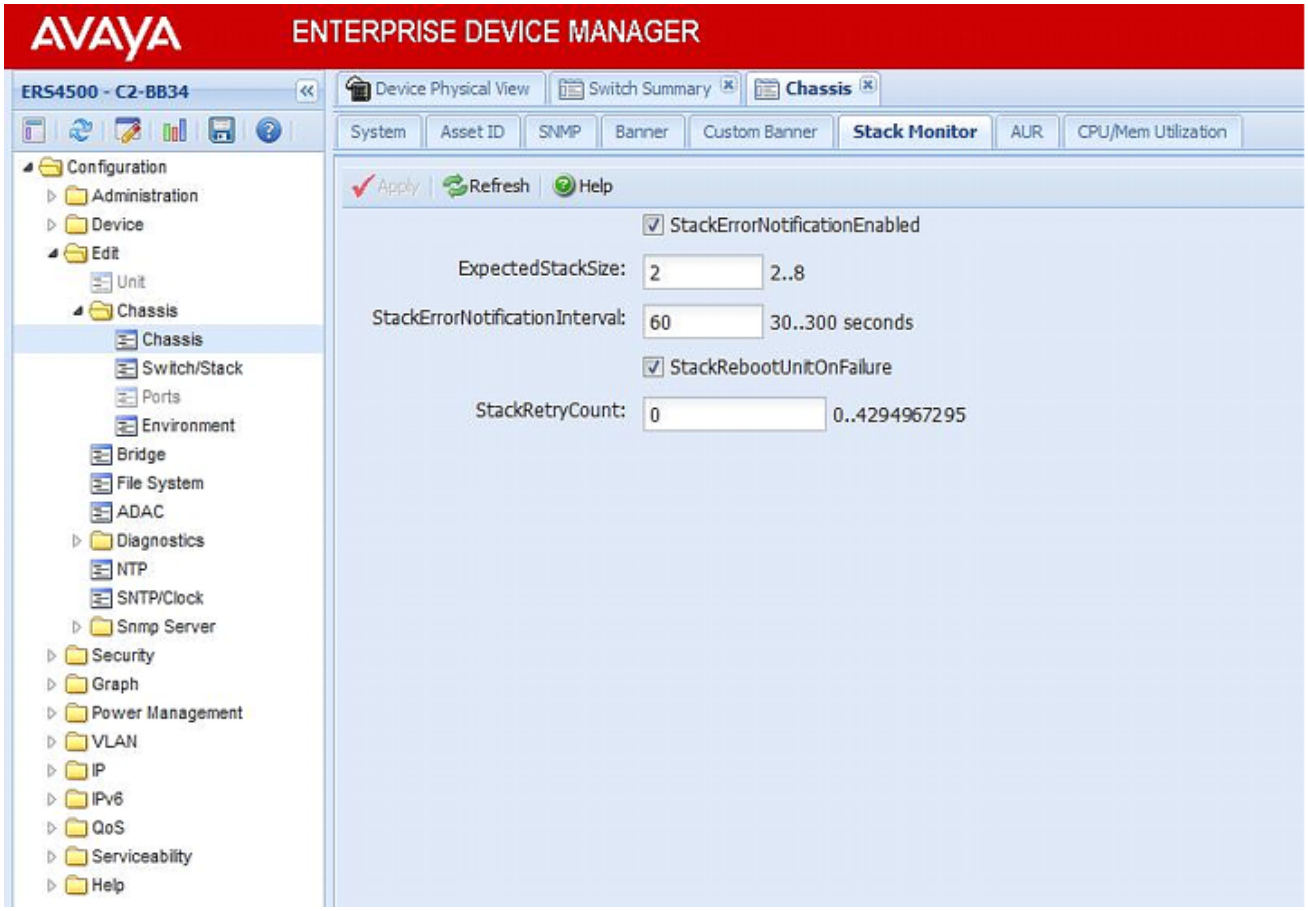


Figure 5: Stack monitor configuration using EDM

Viewing power supply information using EDM

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

The power supply parameters for the PoE switches, PoE4550-T-PWR; and POE45GT, differ slightly because they support Power over Ethernet (PoE).

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 **Environment**.
4. On the work area, click the **PowerSupply** tab.

Variable definitions

Use the data in the following table to help you understand the switch power supply display.

Variable	Value
Unit 1 Primary Power Supply	Indicates the status of primary power supply.
Unit 1 Redundant Power Supply	Indicates the status of redundant power supply.
Important: For a stack environment, this work area displays Primary and Redundant power supply information for each switch unit in the stack.	

Viewing switch fan information using EDM

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

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 **Environment**.
4. On the work area, click the **Fan** tab.

Variable definitions

The following table describes the Fan operating status.

Variable	Value
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.
Important: For a stack environment, this work area displays similar fan information for each switch unit in the stack.	

Viewing switch temperature using EDM

Use the following procedure to display switch temperature 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 **Environment**.
4. In the work area, click the **Temperature** tab.
5. On the tool bar, click **Refresh** to update the data.

Variable definitions

The following table describes the Fan operating status.

Variable	Value
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.

Chassis configuration statistics management using EDM

Use the information in this section to display and graph chassis configuration statistics.

Graphing chassis IP statistics using EDM

Perform this procedure to display and graph switch IP statistics.

Procedure steps

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **IP** tab.
4. On the toolbar, select a **Poll Interval** from the list.
5. On the toolbar, you can click **Clear Counters** to reset the IP statistics counters.
6. To select statistics to graph, click a statistic type row under a column heading.

7. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

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

Variable	Value
InReceives	The total number of input datagrams received from interfaces, including those received in error.
InHdrErrors	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	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	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. For addresses that do not act as IP Gateways, this counter includes only those packets Source-Routed by way of this address with successful Source-Route option processing.
InUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InDiscards	The number of input IP datagrams for which no problems are encountered to prevent their continued processing, but that are discarded (for example, for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.
InDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	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	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that are discarded (for example, for lack of buffer space). This counter can include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
OutNoRoutes	The number of IP datagrams discarded because no route can be found to transmit them to their destination. This counter also includes any packets counted in ipForwDatagrams that have no route. This includes any datagrams a host cannot route because all of its default gateways are down.
FragOKs	The number of IP datagrams successfully fragmented at this entity.

Table continues…

Variable	Value
FragFails	The number of IP datagrams that are discarded because they need to be fragmented at this entity but cannot be, for example, because their Don't Fragment flag was set.
FragCreates	The number of generated IP datagram fragments because of a fragmentation at this entity.
ReasmReqds	The number of IP fragments received that needed to be reassembled at this entity.
ReasmOKs	The number of IP datagrams successfully reassembled.
ReasmFails	The number of failures detected by the IP reassembly algorithm (for example, timed out, errors). This is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC815) can lose track of the number of fragments by combining them as they are received.

Graphing chassis ICMP In statistics using EDM

Use this procedure to display and graph ICMP In statistics.

Procedure steps

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work are, click the **ICMP In** tab.
4. On the toolbar, select a **Poll Interval** from the list.
5. On the toolbar, you can click **Clear Counters** to reset the IP statistics counters.
6. To select statistics to graph, click a statistic type row under a column heading.
7. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

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

Variable	Value
SrcQuenchs	The number of ICMP Source Quench messages received.
Redirects	The number of ICMP Redirect messages received.
Echos	The number of ICMP Echo (request) messages received.
EchoReps	The number of ICMP Echo Reply messages received.
Timestamps	The number of ICMP Timestamp (request) messages received.
TimestampReps	The number of ICMP Timestamp Reply messages received.

Table continues…

Variable	Value
AddrMasks	The number of ICMP Address Mask Request messages received.
AddrMaskReps	The number of ICMP Address Mask Reply messages received.
ParmProbs	The number of ICMP Parameter Problem messages received.
DestUnreachs	The number of ICMP Destination Unreachable messages received.
TimeExcds	The number of ICMP Time Exceeded messages received.

Graphing chassis ICMP Out statistics using EDM

Use this procedure to display and graph ICMP Out statistics.

Procedure steps

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work are, click the **ICMP Out** tab.
4. On the toolbar, select a **Poll Interval** from the list.
5. On the toolbar, you can click **Clear Counters** to reset the IP statistics counters.
6. To select statistics to graph, click a statistic type row under a column heading.
7. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

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

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

Graphing chassis TCP statistics using EDM

Use this procedure to display and graph TCP statistics.

Procedure steps

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **TCP** tab.
4. On the toolbar, select a **Poll Interval** from the list.
5. On the toolbar, you can click **Clear Counters** to reset the IP statistics counters.
6. To select statistics to graph, click a statistic type row under a column heading.
7. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

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

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

Table continues…

Variable	Value
OutRsts	The number of TCP segments sent containing the RST flag.
HCInSegs	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	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 chassis UDP statistics using EDM

Use this procedure to display and graph UDP statistics.

Procedure steps

1. From the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **UDP** tab.
4. On the toolbar, select a **Poll Interval** from the list.
5. On the toolbar, you can click **Clear Counters** to reset the IP statistics counters.
6. To select statistics to graph, click a statistic type row under a column heading.
7. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

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

Variable	Value
InDatagrams	The total number of UDP datagrams delivered to UDP users.
NoPorts	The total number of received UDP datagrams for which there was no application at the destination port.
InErrors	The number of received UDP datagrams that cannot be delivered for reasons other than the lack of an application at the destination port.
OutDatagrams	The total number of UDP datagrams sent from this entity.
HCInDatagrams	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
HCOutDatagrams	The number of UDP datagrams sent from this entity, for devices that can transmit more than 1 million UDP datagrams for each second. Discontinuities in the value of this counter can occur at reinitialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime.

Port configuration statistics management using EDM

Use the information in this section to display and graph port configuration statistics.

Graphing port interface statistics using EDM

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

Procedure steps

1. On the Device Physical View, click a port.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **Interface** tab.
5. On the toolbar, select a **Poll Interval** from the list.
6. On the toolbar, you can click **Clear Counters** to reset the IP statistics counters.
7. To select statistics to graph, click a statistic type row under a column heading.
8. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

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

Variable	Value
InOctets	The total number of octets received on the interface, including framing characters.
OutOctets	The total number of octets transmitted out of the interface, including framing characters.
InUcastPkts	The number of packets delivered by this sublayer to a higher sublayer that are not addressed to a multicast or broadcast address at this sublayer.
OutNUcastPkts	The total number of packets that higher-level protocols requested be transmitted, and that are addressed to a multicast or broadcast address at this sublayer, including those that are discarded or not sent.
InMulticastPkts	The number of packets delivered by this sublayer to a higher sublayer that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both group and functional addresses.
OutMulticastPkts	The number of packets that higher-level protocols requested be transmitted, and that are addressed to a multicast address at this sublayer, including those that were discarded or not sent. For a MAC layer protocol, this number includes both group and functional addresses.

Table continues…

Variable	Value
InBroadcastPkts	The number of packets delivered by this sublayer to a higher sublayer that are addressed to a broadcast address at this sublayer.
OutBroadcastPkts	The number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this sublayer, including those that were discarded or not sent.
InDiscards	The number of inbound packets chosen to be discarded even though no errors were detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet can be to free up buffer space.
OutDiscards	The number of outbound packets chosen to be discarded even though no errors were detected to prevent their being transmitted. One possible reason for discarding such a packet can be to free up buffer space.
InErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
OutErrors	For packet-oriented interfaces, the number of outbound packets that cannot be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that cannot be transmitted because of errors.
InUnknownProtos	For packet-oriented interfaces, the number of packets received through the interface that are discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received through the interface that are discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter is always zero.

Graphing port Ethernet error statistics using EDM

Use this procedure to display and graph Ethernet error statistics.

Procedure steps

1. On the Device Physical View, click a port.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **Ethernet Errors** tab.
5. On the toolbar, select a **Poll Interval** from the list.
6. On the toolbar, you can click **Clear Counters** to reset the IP statistics counters.
7. To select statistics to graph, click a statistic type row under a column heading.
8. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

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

Variable	Value
AlignmentErrors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the AlignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
FCSErrors	A count of frames received on a particular interface that are an integral number of octets in length, but do not pass the FCS check. The count represented by an instance of this object is incremented when the FCSErrors status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
InternalMacTransmitErrors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object.
InternalMacReceiveErrors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object. The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object can represent a count of receive errors on a particular interface that are not otherwise counted.
CarrierSenseErrors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once for each transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
FrameTooLongs	A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the FrameTooLongs status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.

Table continues…

Variable	Value
SQETestErrors	A count of times that the SQE Test Errors message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
DeferredTransmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object.
MultipleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	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	A count of frames for which transmission on a particular interface fails due to excessive collisions.

Graphing port RMON statistics using EDM

Use this procedure to display and graph RMON Ethernet statistics.

Procedure steps

1. On the Device Physical View, click a port.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. Click the **Rmon** tab.
5. On the toolbar, select a **Poll Interval** from the list.
6. On the toolbar, you can click **Clear Counters** to reset the IP statistics counters.
7. To select statistics to graph, click a statistic type row under a column heading.
8. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

Use the data in the following table understand RMON Ethernet statistics.

Variable	Value
Octets	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	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
BroadcastPkts	The total number of good packets received that are directed to the broadcast address. This does not include multicast packets.
MulticastPkts	The total number of good packets received that are directed to a multicast address. This number does not include packets directed to the broadcast address.
CRCAlignErrors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
UndersizePkts	The total number of packets received that are less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
OversizePkts (>1518)	The total number of packets received that are longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
Fragments	The total number of packets received that are less than 64 octets in length (excluding framing bits but including FCS octets) and with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). For etherStatsFragments to increment is normal because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Jabbers	The total number of packets received that are longer than 1518 octets (excluding framing bits, but including FCS octets), with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
1..64	The total number of packets (including bad packets) received that are less than or equal to 64 octets in length (excluding framing bits but including FCS octets).

Table continues…

Variable	Value
65 ..127	The total number of packets (including bad packets) received that are greater than 64 octets in length (excluding framing bits but including FCS octets).
128 ..255	The total number of packets (including bad packets) received that are greater than 127 octets in length (excluding framing bits but including FCS octets).
256..511	The total number of packets (including bad packets) received that are greater than 255 octets in length (excluding framing bits but including FCS octets).
512..1023	The total number of packets (including bad packets) received that are greater than 511 octets in length (excluding framing bits but including FCS octets).
1024..1518	The total number of packets (including bad packets) received that are greater than 1023 octets in length (excluding framing bits but including FCS octets).

Graphing miscellaneous port statistics using EDM

Use this procedure to display and graph miscellaneous statistics for a switch port.

Procedure steps

1. On the Device Physical View, click a port.
2. From the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **Misc.** tab.
5. On the toolbar, select a **Poll Interval** from the list.
6. On the toolbar, you can click **Clear Counters** to reset the IP statistics counters.
7. To select statistics to graph, click a statistic type row under a column heading.
8. On the toolbar, click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

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

Variable	Value
NoResourcesPktsDropped	The number of packets dropped due to switch memory shortage.

Chapter 10: RMON configuration using Enterprise Device Manager

This chapter describes the procedure you can use to configure and manage RMON using the Enterprise Device Manager (EDM).

Prerequisites

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

RMON history management using EDM

Use the information in this section to display, create, and delete RMON history characteristics.

Viewing RMON history using EDM

Ethernet history records periodic statistical samples from a network. A sample is called a history and is gathered in time intervals referred to as buckets.

Histories establish a time-dependent method for gathering RMON statistics on a port. The default values for history are the folowing:

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

You can configure the time interval and the number of buckets. However, when the last bucket is reached, bucket 1 is dumped and recycled to hold a new bucket of statistics. Then, bucket 2 is dumped, and so forth.

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. On the work area, click the **History** tab to view the history.

Variable definitions

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

Variable	Value
Index	A unique value assigned to each interface. An index identifies an entry in a table.
Port	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.
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. The actual number of buckets associated with this entry can be 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.
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 any number of seconds between 1 and 3600 (1 hour). Because the counters in a bucket can overflow at their maximum value with no indication, note the possibility of overflow in any of the associated counters. Consider the minimum time in which any counter could overflow on a particular media type and set the historyControlInterval object to a value less than this interval. This minimum time is typically most important for the octets counter in any media-specific table. For example, on an Ethernet network, the etherHistoryOctets counter could overflow in about 1 hour at the maximum utilization of the Ethernet.
Owner	Indicates the network management system that created this entry.

Creating RMON history characteristics using EDM

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

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

Procedure steps

1. From the navigation tree, double-click **Rmon**.
2. In the RMON tree, double-click **Control**.
3. In the work area, click **Insert** to open the Insert History dialog.

4. Type the port number or click the ellipsis to select a port from the list.
5. In the **Buckets Requested** box, type the number of buckets, or click the ellipsis to select a value from the list. The default value is 50.
6. In the **Interval** box, type the length of the interval or click the ellipsis to select a value from the list. The default value is 1800.
7. In the **Owner** box, type the owner— the network management system that created this entry.
8. Click **Insert** to add the entry to the list and return to the History tab.

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

Variable definitions

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

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

Disabling RMON history using EDM

Use 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. On the work area, click the **History** tab to view the history.
5. In the table, select the row that you want to delete.
6. On the toolbar, click **Delete**.

Viewing RMON history statistics using EDM

Use the following procedure to display RMON history statistics:

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 **Serviceability**.
2. In the Serviceability tree, double-click **RMON**.
3. In the RMON tree, double-click **Control**.
4. On the work area, click the **History** tab to view the history.
5. In the table, select a port row.
6. On the toolbar, click **Display History Data**.

Variable definitions

Use the data in the following table to help you understand the RMON history statistics display.

Variable	Value
SampleIndex	The sample number. As history samples are taken, they are assigned greater sample numbers.
Utilization	Estimate the percentage of the capacity of a link that is used during the sampling interval.
Octets	The number of octets received on the link during the sampling period.

Table continues…

Variable	Value
Pkts	The number of packets received on the link during the sampling period.
BroadcastPkts	The number of packets received on the link during the sampling interval that destined for the packet address.
MulticastPkts	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	The number of received packets that are dropped because of system resource constraints.
CRCAlignErrors	The number of packets received during a sampling interval that are between 64 and 1518 octets long. This length includes 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 nonintegral number of octets (Alignment Error).
UndersizePkts	The number of packets received during the sampling interval are less than 64 octets long (including FCS octets, but not framing bits).
OversizePkts	The number of packets received during the sampling interval are longer than 1518 octets (including FCS octets, but not framing bits, and are otherwise well formed).
Fragments	The number of packets received during the sampling interval are 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 nonintegral number of octets (Alignment Error).
Collisions	The best estimate of the number of collisions on an Ethernet segment during a sampling interval.

RMON Ethernet statistics management using EDM

Use the information in the following sections to manage RMON Ethernet statistics.

Viewing RMON Ethernet statistics 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. On the work area, click the **Ether Stats** tab to view the history.

Variable definitions

Use the data in the following table help you understand the RMON Ethernet statistics display.

Variable	Value
Owner	The network management system that created this entry.
Index	A unique value assigned to each interface. An index identifies an entry in a table.
Port	A port on the device.
DropEvents	The number of received packets that are dropped because of system resource constraints.
Octets	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	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
BroadcastPkts	The total number of good packets received that are directed to the broadcast address. This does not include multicast packets.
MulticastPkts	The total number of good packets received that are directed to a multicast address. This number does not include packets directed to the broadcast address.
CRCAlignErrors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
UndersizePkts	The total number of packets received that are less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
OversizePkts (>1518)	The total number of packets received that are longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
Fragments	The total number of packets received that are less than 64 octets in length (excluding framing bits but including FCS octets) and with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). For etherStatsFragments to increment is normal because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Jabbers	The total number of packets received that are longer than 1518 octets (excluding framing bits, but including FCS octets), with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.

Table continues…

Variable	Value
1..64	The total number of packets (including bad packets) received that are less than or equal to 64 octets in length (excluding framing bits but including FCS octets).
65 ..127	The total number of packets (including bad packets) received that are greater than 64 octets in length (excluding framing bits but including FCS octets).
128 ..255	The total number of packets (including bad packets) received that are greater than 127 octets in length (excluding framing bits but including FCS octets).
256..511	The total number of packets (including bad packets) received that are greater than 255 octets in length (excluding framing bits but including FCS octets).
512..1023	The total number of packets (including bad packets) received that are greater than 511 octets in length (excluding framing bits but including FCS octets).
1024..1518	The total number of packets (including bad packets) received that are greater than 1023 octets in length (excluding framing bits but including FCS octets).

Enabling RMON 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. On the work area, click the **Ether Stats** tab to view the history.
5. On the toolbar, click **Insert**.
6. Type an index in the **Index** field.
7. Click the Port ellipses (**...**), and select the port you want to use.
8. Type the owner name in the **Owner** field.
9. Click **Insert**.

Variable definitions

Use the data in the following table to enable RMON Ethernet statistics gathering.

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

Disabling RMON Ethernet statistics gathering using EDM

Use this procedure to disable 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. On the work area, click the **Ether Stats** tab to view the history.
5. On the toolbar, select the port row you want to delete.
6. On the toolbar, click **Delete**.

RMON alarm management using EDM

This section describes the procedures you can use to use the alarm manager.

Viewing RMON alarm configuration information using EDM

Use the following procedure to create an alarm for receiving 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. On the work area, click the **Alarms** tab.

Variable definitions

Use the data in the following table to help you understand the RMON alarm display.

Variable	Value
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. Range is 1–65535.
Interval	Time period (in seconds) over which the data is sampled and compared with the rising and falling thresholds.
Variable	Name and type of alarm—indicated by the format: • *alarmname.x* where x=0 indicates a chassis alarm. • *alarmname*. where you must specify the index. This 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 displays in the port selection tool.
Sample Type	Specifies the sample type—absolute or delta.
Value	Indicates the value of the alarm statistic during the last sampling period, compared with the rising and falling thresholds.
StartupAlarm	Indicates the type of alarm generated at startup, based on rising and falling thresholds. Values include: • risingAlarm • risingOrFallingAlarm • fallingAlarm
RisingThreshold	When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, generates a single event.
RisingEventIndex	Index of the event entry that is used when 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.)
FallingThreshold	When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, generates a single event.
FallingEventindex	Index of the event entry that is used when 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	Specifies the owner name.
Status	Indicates the status of the alarm entry.

Creating an RMON alarm using EDM

Use the following procedure to create an alarm for receiving 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. On the work area, click the **Alarms** tab to view the history.
5. On the toolbar, click **Insert**.
6. Configure the parameters as required.
7. Click **Insert**.

Variable definitions

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

Variable	Value
Variable	Name and type of alarm—indicated by the format: • *alarmname.x* where x=0 indicates a chassis alarm. • *alarmname*. where you must specify the index. This 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 displays in the port selection tool.
Sample Type	Specifies the sample type—absolute or delta.
Interval	Specifies the time period (in seconds) over which the data is sampled and compared with the rising and falling thresholds.
Index	Uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device. Range is 1–65535.
RisingThreshold	When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, generates a single event.
RisingEventIndex	Specifies the index of the event entry that is used when 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.)

Table continues…

Variable	Value
FallingThreshold	When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, generates a single event.
FallingEventindexSpecifies the	Specifies the index of the event entry that is used when 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	Specifies the owner name.

Deleting an RMON alarm using EDM

Use this procedure to delete an alarm:

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. On the work area, click the **Alarms** tab.
5. In the table, select the alarm you want to delete.
6. On the toolbar, click **Delete**.
7. Click **Yes**.

Event management using EDM

This section describes the procedures you can use to configure RMON events and alarms work together to provide notification when values in the network are outside of a specified range. When values pass the specified ranges, the alarm is triggered. The event specifies how the activity is recorded.

Prerequisites

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

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. On the work area, click the **Events** tab to view the history.

Variable definitions

The following table describes the Events tab fields.

Variable	Value
Index	This index uniquely identifies an entry in the event table. Each entry defines one event that is to be generated when the appropriate conditions occur.
Description	Specifies whether the event is a rising or falling event.
Type	The type of notification that the switch 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 follow: • none • log • trap • log-and-trap
Community	The SNMP community string acts as a password. Only those management applications with this community string can view the alarms.
LastTimeSent	The value of sysUpTime at the time this event entry last generated an event. If this entry has not generates any events, this value is zero.
Owner	If traps are specified to be sent to the owner, this is the name of the machine that receives alarm 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. On the work area, click the **Events** tab to view the history.
5. On the toolbar, click **Insert**.

   The Insert Events dialog box appears.
6. Type an index in the **Index** field.
7. Type the name of the event in the **Description** field.
8. Choose the type of the event in the **Type** field.
9. Type the community information in the **Community** field.
10. Type the owner information in the **Owner** field.
11. Click **Insert**.

Deleting an event using EDM

Use this 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. On the work area, click the **Events** tab to view the history.
5. In the table, select the event row you want to delete.
6. On the toolbar, click **Delete**.

Managing log information management using EDM

Use the information in this procedure to chronicle and describe alarm activity.

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 **Serviceability**.
2. In the Serviceability tree, double-click **RMON**.
3. In the RMON tree, double-click **Alarms**.
4. On the work area, click the **Log** tab to view the history.

Variable definitions

The following table describes the Log tab fields.

Variable	Value
Time	Specifies when an event occurs that activats the log entry.
Description	Specifies whether the event is a rising or falling event.
EventIndex	Specifies the event index.

Chapter 11: Network monitoring configuration using Enterprise Device Manager

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

Prerequisites

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

Viewing CPU and memory utilization using EDM

Use the following procedure to view both 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. In the work area, click the **CPU/Mem Utilization** tab.
5. On the tool bar, click **Refresh** to update the data.

Variable definitions

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

Variable	Value
Unit	Indicates the numerical representation of 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 CPU usage in percentage, since system start up.
MemoryTotalMB	Indicates the total memory present, in megabytes, on the unit.
MemoryAvailableMB	Indicates the memory remaining available on the unit.
MemoryUsedMB	Indicates the memory being used on the unit.

Switch stack information management using EDM

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

Viewing stack information using EDM

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

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. On the work area, click the **Stack Info** tab.

Variable Definitions

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

Variable	Value
Indx	Indicates the line number for stack info.

Table continues…

Variable	Value
Descr	Describes the component or subcomponent. If not available, the value is a zero length string.
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	Indicates the state of the component or subcomponent. • enable: enables operation • reset: resets component
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 The component type determines the allowable (and meaningful) values.

Table continues…

Variable	Value
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 using EDM

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

Procedure steps

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

Variable definitions

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

Variable	Value
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

Table continues…

Variable	Value
	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. 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.

Table continues…

Variable	Value
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.
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 using EDM

Use this procedure to display pluggable port information.

Procedure steps

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

Variable definitions

Use the data in the following table to help you understand the pluggable ports display.

Variable	Value
Unit	Identifies the unit number.
Port	Identifies the number of the pluggable port.

Table continues…

Variable	Value
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.
DateCode	Identifies the date code.
VendorData	Identifies vendor data.
OrderCode	Identifies the order code.

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.
Unit	Indicates the unit number.
Description	Describes each unit in the stack.
Cascade Up	Indicates the cascade up link status.

Table continues…

Variable	Value
Cascade Down	Indicates the cascade down link status.
Stack Role	Indicates which unit is the base unit.

Configuring the system log using EDM

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

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 **Diagnostics**.
3. In the Diagnostics tree, double-click **System Log**.
4. In the work area, click the **System Log Settings** tab.
5. Choose the operation in the **Operation** field.
6. Choose the buffer space allocation in the **BufferFullAction** field.
7. Choose the type of system messages to save in volatile memory in the **SaveTargets**field.
8. Choose the type of system messages to save in non-Volatile memory in the **SaveTargets** field.
9. Choose the types of system log messages to delete from volatile and non-volatile memory in the **ClearMessageBuffers** field.
10. On the tool bar, Click **Apply**.

Variable definitions

Use the data in the following table to configure the system log.

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

Table continues…

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).
Volatile - CurSize	Indicates the number of messages currently stored in volatile memory.
Volatile - SaveTargets	Specifies the type of system messages to save in volatile memory. • critical—only messages classified as critical are saved in volatile memory • critical/serious—only messages classified as critical and serious are saved in volatile memory • critical/serious/inform—only messages classified as critical, serious, andinformational are saved in volatile memory • none—no system log messages are saved in volatile memory
non-Volatile - CurSize	Indicates the number of messages currently stored in non-volatile memory.
non-Volatile - SaveTargets	Specifies the type of system messages to save in non-volatile memory. • critical—only messages classified as critical are saved in volatile memory • critical/serious—only messages classified as critical and serious are saved in non-volatile memory • critical/serious/inform—only messages classified as critical, serious, andinformational are saved in non-volatile memory • none—no system log messages are saved in volatile memory
ClearMessageBuffers	Specifies the types 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

Table continues…

Variable	Value
	• nonVolSerious—only messages classified as serious are deleted from non-volatile memory

Configuring remote system logging using EDM

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

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 **Diagnostics**.
3. In the Diagnostics tree, double-click **System Log**.
4. In the work area, click the **Remote System Log** tab.
5. Choose the type of IP address of the remote system log server in the **RemoteSyslogAddressType** field.
6. In the **RemoteSyslogAddress** box, enter a IP address of the remote system log server to send system log messages.
7. Choose the type of IP address of the secondary remote system log server in the **SecondarySyslogAddressType** field.
8. In the **SecondarySyslogAddress** box, enter a IP address of the secondary remote system log server to send system log messages.
9. Choose the **Enabled** checkbox to enable remote system logging.

   OR

   Clear the **Enabled** checkbox to disable remote system logging.
10. In the**Save Targets** section, click the type of system messages.
11. In the **Facility** section, click the type of facility required.
12. On the toolbar, click **Apply**.

Variable definitions

Use the data in the following table to 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 send system log messages to.
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
Facility	Specifies the remote logging facility. • Daemon • Local0 • Local1 • Local2 • Local3 • Local4 • Local5 • Local6 • Local7 DEFAULT: Daemon

Viewing system logs using EDM

Use the following procedure to display system log information.

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 **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.

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
- Configuring Port Mirroring using EDM

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

The following table describes the Port Mirrors tab fields.

Variable	Value
Instance	Specifies the numerical assignment of the port mirroring (1-4)
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.
RspanVlan	Specifies the RspanVlan to be associated with a source port-mirroring instance.

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

Variable definitions

The following table describes the Port Mirrors tab fields.

Variable	Value
Instance	Indicates the Port Mirroring instance number (1-4)
Port Mode	Indicates the supported Port Mirroring modes. The modes are: • Adst—Mirror packets with destination MAC address A.

Table continues…

Variable	Value
	• 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 packets received on port Y and transmitted on port X. • Xtx—Mirror packets transmitted on port X. The default value is Disabled.
Monitor Port	Specifies the monitoring 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.

Table continues…

Variable	Value
AllowTraffic	Indicates whether bi-directional mirroring traffic is enabled.
RspanVlan	Specifies the RspanVlan to be associated with a source port-mirroring instance.

Chapter 12: IPFIX configuration using Enterprise Device Manager

This chapter describes the procedures you can use to configure IP Flow Information Export (IPFIX) using Enterprise Device Manager (EDM).

Prerequisites

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

Configuring IPFIX globally using EDM

Use the following procedure to enable or disable IPFIX for the switch. IPFIX is disabled by default.

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 **Serviceability**.
2. In the Serviceability tree, double-click **IPFIX**.
3. In the work area, click the **Global** tab.
4. In the State section, click the **enable** radio button to enable IPFIX globally.

   OR

   Click the **disable** radio button to disable IPFIX globally.

5. Click **Apply**.

Configuring IPFIX flows using EDM

Use the following procedure to configure export flow information sources.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **IPFIX**.
3. In the work area, click the **Exporters** tab.
4. To select an exporter to edit, click the exporter slot number.
5. In the exporter row, double-click the cell in the **AgingIntv** column.
6. Type a value in the dialog box.
7. In the exporter row, double-click the cell in the **ExportState** column.
8. In the exporter row, double-click the cell in the **ExportIntv** column.
9. Select a value from the list.
10. In the exporter row, double-click the cell in the **TempRefIntvSec** column.
11. Type a value in the dialog box.
12. In the exporter row, double-click the cell in the **TempRefIntvPkts** column.
13. Type a value in the dialog box.
14. Click **Apply**.

Variable definitions

Variable	Value
Slot (Unit)	Identifies the switch that is exporting IPFIX flows. This value corresponds to the unit number in a stack or is the number 1 for a stand-alone unit.
AgingIntv	Specifies the aging interval of the flow record in seconds. Values range from 0–2147400 seconds. Aging time is the period of time in which all records are verified if they are updated. The records are

Table continues…

Variable	Value
	deleted if no new updates are found between two checks.
ActiveTimeout	Indicates the flow record active timeout value in minutes. This is a read-only cell.
ExportIntv	Specifies the frequency of data exports to the collector in seconds. Values range from 10 to 3600 seconds.
ExportState	Enables or disables the exporter.
TempRefIntvSec	Specifies the template refresh timeout in seconds. Values range from 300 to 3600. The template is sent out to the collector either at the configured interval or after the specified template packets refresh number is reached, whichever occurs first.
TempRefIntvPkts	Specifies the template refresh timeout in numbers of packets. Values range from 10000 to 100000 packets. The template is sent out to the collector either after the configured template packets refresh number is reached or at the specified refresh interval, whichever occurs first.

IPFIX collector management using EDM

Use the information in this section to display configured IPFIX collector information and to modify IPFIX collector configurations.

Viewing IPFIX collectors using EDM

Use the following procedure to display collected and analyzed data exported from an IPFIX-compliant switch.

Procedure steps

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

Variable definitions

Variable	Value
Slot (Unit)	Identifies the switch that is collecting and analyzing data. This value corresponds to the unit number in a stack or is the number 1 for a stand-alone unit.
AddressType	Indicates the IP address type 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.
DestPort	Indicates the port on which the collector is listening for IPFIX data. Currently only port 9995 is supported.
ProtoVer	Indicates the format in which IPFIX data is provided to the collector. Currently only Netflow version 9 formatting is supported.
Enable	Indicates the operational state of this collector.

Configuring IPFIX collectors using EDM

Use the following procedure to collect and analyze data exported from an IPFIX-compliant switch.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **IPFIX**.
3. In the work area, click the **Collectors** tab.
4. Click the **Insert**.
5. In the Slot dialog box, type a value.
6. In the Address dialog box, type an IP address.
7. Select the **Enable** check box to enable the collector.

   OR

   Clear the **Enable** check box to disable the collector.
8. Click **Apply**.

Variable definitions

Variable	Value
Slot (Unit)	Identifies the switch that is collecting and analyzing data. This value corresponds to the unit number in a stack or is the number 1 for a stand-alone unit.
AddressType	Specifies the IP address type of the collector. Currently only IPv4 addresses are supported.
Address	Specifies the IP address of the collector.
Protocol	Specifies the protocol used to transport the IPFIX data to the collector. Currently only the UDP protocol is supported for this task.
DestPort	Specifies the port on which the collector is listening for IPFIX data. Currently only port 9995 is supported.
ProtoVer	Specifies the format in which IPFIX data is provided to the collector. Currently only Netflow version 9 formatting is supported.
Enable	Enables or disables the collector.

Deleting IPFIX collectors using EDM

Use the following procedure to display collected and analyzed data exported from an IPFIX-compliant switch.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **IPFIX**.
3. In the work area, click the **Collectors** tab.
4. To select an collector to delete, click the collector slot number.
5. Click **Delete**.

IPFIX port management using EDM

Use the information in this section to view and modify IPFIX port configurations.

Viewing IPFIX port information using EDM

Use the following procedure to display IPFIX port configuration information.

Procedure steps

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

Variable definitions

Variable	Value
Id	Indicates the individual port on which the IPFIX parameters are being configured. Ports are itemized in the Unit/Port format.
Flush	Indicates the flushing action to take on the port. Flushing the port of data involves deleting all previously gathered information about that port. Values include: • none—the port data is not flushed. • flush—the port data is flushed, which deletes the data from switch memory. • exportAndFlush—the port data is exported to a configured collector and the data is then flushed.
AllTraffic	Indicates if IPFIX data is collected on this port. • enable—IPFIX data is collected • disable—IPFIX data is not collected

Modifying specific IPFIX port configurations using EDM

Use the following procedure to modify IPFIX configuration parameters for specific ports.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **IPFIX**.
3. In the work area, click the **Ports** tab.
4. In the port row, double-click the cell in the **Flush** column.
5. Select a value from the list.
6. In the port row, double-click the cell in the **AllTraffic** column.
7. Select a value from the list.
8. Repeat steps **4** through **8** to modify additional ports.
9. Click **Apply**.

Variable definitions

Variable	Value
Id	Specifies the individual port on which the IPFIX parameters are being configured. Ports are itemized in the Unit/Port format.
Flush	Specifies the flushing action to take on the port. Flushing the port of data involves deleting all previously gathered information about that port. Values include: • none—the port data is not flushed. • flush—the port data is flushed, which deletes the data from switch memory. • exportAndFlush—the port data is exported to a configured collector and the data is then flushed.
AllTraffic	Specifies if IPFIX data is collected on this port. • enable—IPFIX data is collected • disable—IPFIX data is not collected

Modifying all IPFIX port configurations using EDM

Use the following procedure to modify the IPFIX configuration parameters for all available ports.

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **IPFIX**.
3. In the work area, click the **Ports** tab.
4. Click **Multi-Select**.
5. In the Make Selection, **Items** section, select a checkbox to make the corresponding item in the Values section available to configure.
6. In the Values, **Flush** section, select a radio button.
7. In the Values, **AllTraffic** section, select a radio button.
8. Click **Ok**.
9. Click **Apply**.

Variable definitions

Variable	Value
Flush	Specifies the flushing action to take on the port. Flushing the port of data involves deleting all previously gathered information about that port. Values include: • none—the port data is not flushed. • flush—the port data is flushed, which deletes the data from switch memory. • exportAndFlush—the port data is exported to a configured collector and the data is then flushed.
AllTraffic	Specifies if IPFIX data is collected on this port. • enable—IPFIX data is collected • disable—IPFIX data is not collected

Displaying IPFIX data information using EDM

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.

Variable definition

Name	Description
Unit Number	Specifies a standalone switch or a switch that is part of a stack. For a standalone switch, use a value of 1. A value greater than 1 specifies the switch location in a stack.
Sort By	Specifies a rule to sort data by. Values include: • **Source Address** : source IP address • **Destination Address** : destination IP address

Table continues…

Name	Description
	• **Protocol** : protocol number • **TOS** : type of service • **Port** : port number • **TCP/UDP Src Port** : TCP/UDP source port • **TCP/UDP Dest Port** : TCP/UDP destination port • **Packet Count** : packet number • **Byte Count** : data byte number • **First Packet Time** : first packet time • **Last Packet Time** : last packet time Default: Source Address
Sort Order	Specifies the order in which to sort data. Values include: • **Ascending** • **Descending** Default: Ascending
Display	Specifies the number of entries to display. Values include: • **Top 10** : displays first 10 entries • **Top 25** : displays first 25 entries • **Top 50** : displays first 50 entries • **Top 100** : displays first 100 entries • **Top 200** : displays first 200 entries Default: Top 50

Graphing IPFIX exporter statistics for a collector using EDM

Use the following procedure to graph collected and analyzed data exported from an IPFIX-compliant switch.

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 **Serviceability**.
2. In the Serviceability tree, double-click **IPFIX**.
3. In the work area, click the **Collectors** tab.
4. Click **Graph**.
5. Click the **Exporter** tab.
6. To select collector data to graph, click any column in either the **OutPkts**, **OutOctets**, or **PktsLoss** row.
7. From the **Poll Interval** list, select an interval.
8. Click a **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Variable definitions

Variable	Value
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 using EDM

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

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 **Serviceability**.
2. In the Serviceability tree, double-click **IPFIX**.
3. In the work area, click the **Collectors** tab.

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

Chapter 13: SLA Monitor Configuration using Enterprise Device Manager

A server is required to fully utilize the capabilities of the SLA Monitor agent. The agent can be used without a server.

The SLA Monitor agent must be enabled to run specific QoS tests in the absence of an SLA Monitor server. Agents exchange packets between one another to conduct the QoS tests. SLA Monitor uses Real Time Protocol (RTP) and New Trace Route (NTR) tests to determine QoS benchmarks.

Note:

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

Use the following procedures to configure SLA Monitor using EDM

Related Links

Configuring SLA Monitor using EDM on page 160

Configuring SLA Monitor using EDM

Use this procedure to configure SLA Monitor.

Procedure

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

Variable definition

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.
ServerBypass	Enables or disables the SLA Monitor agent server bypass mode. • **enabled**: enables the SLA Monitor agent server bypass mode. • **disabled**: disables the SLA Monitor agent server bypass mode.
RefuseServerTests	Enables or disables the NTR and RTP test requests from the server. • **enabled**: the SLA Monitor agent rejects test requests from the server with which it is registered. • **disabled**: the SLA Monitor agent server accepts test requests from the server with which it is registered. Test requests originating from platform, SLM CLI interfaces, and SNMP are not affected.
ConfiguredAgentToAgentPort	Specifies the UDP port utilized by the SLA Monitor agent for agent-agent communication. If the value of this attribute is zero, the SLA Monitor agent utilizes 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 causes 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.

Table continues…

Name	Description
	The server must use the same port.
CliAvailable	Specifies whether SLA Monitor agent CLI is available or not available.
CliTimeout	Specifies the maximum amount of time, in seconds, until the CLI session is automatically terminated. The value of this attribute is pertinent only if CLI timeouts are enabled. The default is 60 seconds.
CliTimeoutMode	Configures whether the agent automatic CLI session timeout is enabled or disabled.
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 IP address of the SLA Monitor server with which the agent is registered. This is a read-only field.
RegisteredServerPort	Indicates the TCP port used by the SLA Monitor server with which the agent is registered. This is a read-only field.
RegistrationTime	Indicates the time in seconds since the agent is registered with the server. This is a read-only field.

Table continues…

Name	Description
AgentToAgentPort	Indicates the base UDP port used by the SLA Monitor agent for agent-to-agent communication. The base UDP port is used to derive multiple agent communication ports. This is a read-only field.
EncryptionSupport	Indicates if encrypted agent-server communication is supported.

Executing NTR test using EDM

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

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 steps

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 **NTR**.
4. In the NTR work area, click **Insert** to enter parameters for the new test.
5. In the **OwnerId** dialog box, type the owner id.
6. In the **TestName** dialog box, type the test name.
7. In the **TargetAddress** dialog box, type the target IP address.
8. In the **Dscp** dialog box, type the dscp value.
9. In the **Attempts** dialog box, type the number of attempts.
10. In the **Period** dialog box, type the duration in microseconds.
11. In the **Label** dialog box, type the label.
12. Click **enabled** to enable the administrator status.
13. Click **Insert** to initiate the NTR test.
14. In the NTR work area, click **Results** to view the test results.

Variable definition

Variable	Value
OwnerId	Specifies the owner of an NTR test.
TestName	Specifies the name of an NTR test.
TargetAddress	Specifies the target IP address for the NTR test.

Table continues…

Variable	Value
Dscp	Specifies the Differential Services Code Point (DSCP) value for use in packets that are generated by the NTR test. The value ranges from 0 to 63.
Attempts	Specifies the number of attempts generated by the NTR test. The value ranges from 1 to 10. The default value is 2.
Period	Specifies the interval between packets in microseconds, generated by the NTR test. The value ranges from 10000 to 200000. The default interval is 20000 microseconds.
Label	Specifies the text label used to reference the NTR control entry.
AdminStatus	Specifies the administrator status. You must enable the administrator status to initiate the NTR test. The administrator status is disabled by default.

Viewing NTR test results

Use this procedure to view the NTR test results.

Before you begin

You must execute the NTR test before you view the results.

Procedure

1. In the navigation tree, double-click **Serviceability** .
2. In the Serviceability tree, click **SLA Monitor** .
3. In the SLA Montior work area, click **NTR** .
4. In the NTR work area, click to select the saved test and then click **Results** .
5. In the results work area, click **NTR Results** to view the NTR test results.

Variable definition

Name	Description
HopIndex	Indicates the hop index for an NTR test hop.
TgtAddress	Indicates the IP address associated with the NTR test hop.
Rtt	Indicates the round-trip-time of an NTR test in milliseconds.
IngressDscp	Indicates the DSCP value in the NTR test packet received by the end station for the specified hop.
EgressDscp	Indicates the DSCP value in the NTR test packet received by the SLA Monitor agent for the specified hop.

Executing RTP test using EDM

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

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.

Note:

The ServerBypass must be enabled on the target to complete the test successfully.

Procedure steps

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 **RTP**.
4. In the RTP work area, click **Insert** to enter parameters for the new test.
5. In the **OwnerId** dialog box, type the owner id.
6. In the **TestName** dialog box, enter the test name.
7. In the **TargetAddress** dialog box, type the target IP address.
8. In the **Dscp** dialog box, type the dscp value.
9. In the **TestPackets** dialog box, type the number of test packets.
10. In the **SyncPackets** dialog box, type the number of synchronization packets.
11. In the **Period** dialog box, type the duration in microseconds.
12. Click **enabled** to enable the administrator status.
13. In the **Label** dialog box, type the label.
14. Click **Insert** to initiate the RTP test.
15. In the RTP work area, click **Results** to view the test results.

Variable Definition

Variable	Value
OwnerId	Specifies the owner of an RTP test.
TestName	Specifies the name of an RTP test.
TargetAddress	Specifies the target IP address for the RTP test.
Dscp	Specifies the Differential Services Code Point (DSCP) value for use in packets that are generated by the RTP test. The value ranges from 0 to 63.

Table continues…

Variable	Value
TestPackets	Specifies the number of test packets generated by the RTP test. Test packets are used to determine jitter. The value ranges from 10 to 100.
SyncPackets	Specifies the number of synchronization packets generated by the RTP test. Synchronization packets are used to determine network delay. The value ranges from 10 to 100.
Period	Specifies the interval between packets in microseconds, generated by the RTP test. The value ranges from 10000 to 200000. The default interval is 20000 microseconds.
Label	Specifies the text label used to reference the RTP control entry.
AdminStatus	Specifies the administrator status. You must enable the administrator status to initiate the RTP test. The administrator status is disabled by default.

Viewing real time protocol test results

Use this procedure to view the RTP test results.

Before you begin

You must execute the RTP test before you view the results.

Procedure

1. In the navigation tree, double-click **Serviceability** .
2. In the Serviceability tree, click **SLA Monitor** .
3. In the SLA Montior work area, click **RTP** .
4. In the RTP work area, click to select the saved test and then click **Results** to view the RTP test results.

Variable definitions

Name	Description
OperStatus	Indicates the status of an RTP test. • **inProgess** indicates that an RTP test is in progress. • **aborted** indicates that an RTP test is aborted. • **completed** indicates that an RTP 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.

Table continues…

Name	Description
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 – JitterQuartile5	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.
AbortData	Indicates the details of the RTP test that was aborted.

ACLI

Avaya Command Line Interface (ACLI) is a text-based, common command line interface used for device configuration and management across Avaya products.

application-specific integrated circuit (ASIC)

An application-specific integrated circuit developed to perform more quickly and efficiently than a generic processor.

base unit (BU)

When you connect multiple switches into a stack, one unit, and only one unit, must be designated as a base unit to perform stack configuration tasks. The position of the unit select switch, on the back of the switch, determines base unit designation.

Bridge Protocol Data Unit (BPDU)

A data frame used to exchange information among the bridges in local or wide area networks for network topology maintenance.

cascade down

Refers to the stack configuration. The system automatically numbers the physical units based on the designated base unit, which is Unit 1. In the cascade down configuration, the base unit is physically located on the top of the stack and stacking cables are connected in the appropriate order.

cascade up

Refers to the stack configuration. The system automatically numbers the physical units based on the designated base unit, which is Unit 1. In the cascade up configuration, the base unit is physically located on the bottom of the stack and stacking cables are connected in the appropriate order.

Distributed MultiLink Trunking (DMLT)

A point-to-point connection that aggregates similar ports from different modules to logically act like a single port, but with the aggregated bandwidth.

Enterprise Device Manager (EDM)

A Web-based embedded management system to support single-element management. EDM provides complete configuration management functionality for the supported devices and is supplied to the customer as embedded software in the device.

Frame Check Sequence (FCS)

Frames are used to send upper-layer data and ultimately the user application data from a source to a destination.

Internet Control Message Protocol (ICMP)

A collection of error conditions and control messages exchanged by IP modules in both hosts and gateways.

Internet Group Management Protocol (IGMP)

IGMP is a host membership protocol used to arbitrate membership in multicast services. IP multicast routers use IGMP to learn the existence of host group members on their directly attached subnets.

Internet Protocol Flow Information eXport (IPFIX)

An IETF standard that improves the Netflow V9 protocol. IPFIX monitors IP flows.

Internet Protocol version 4 (IPv4)

The protocol used to format packets for the Internet and many enterprise networks. IPv4 provides packet routing and reassembly.

Internet Protocol version 6 (IPv6)

An improved version of the IP protocol, IPv6 improves the IPv4 limitations of security and user address numbers.

light emitting diode (LED)

A semiconductor diode that emits light when a current passes through it.

Link Aggregation

Provides the mechanism to create and manage trunk groups automatically using Link Aggregation Control Protocol (LACP).

Link Aggregation Control Protocol (LACP)

A network handshaking protocol that provides a means to aggregate multiple links between appropriately configured devices.

Link Aggregation Control Protocol Data Units (LACPDU)

Link aggregation control protocol data unit (LACPDU) is used for exchanging information among LACP-enabled devices.

link aggregation group (LAG)

A group that increases the link speed beyond the limits of one single cable or port, and increases the redundancy for higher availability.

Logical Link Control (LLC)

A protocol used in LANs to transmit protocol data units between two end stations. This LLC layer addresses and arbitrates data exchange between two endpoints.

management information base (MIB)

The MIB defines system operations and parameters used for the Simple Network Management Protocol (SNMP).

mask

A bit string that the device uses along with an IP address to indicate the number of leading bits in the address that correspond with the network part.

media

A substance that transmits data between ports; usually fiber optic cables or category 5 unshielded twisted pair (UTP) copper wires.

Media Access Control (MAC)

Arbitrates access to and from a shared medium.

mirrored port

The port to mirror. The port is also called the source port.

mirroring port

The port to which the system mirrors all traffic, also referred to as the destination port.

MultiLink Trunking (MLT)

A method of link aggregation that uses multiple Ethernet trunks aggregated to provide a single logical trunk. A multilink trunk provides the combined bandwidth of multiple links and the physical layer protection against the failure of a single link.

multiplexing

Carriage of multiple channels over a single transmission medium; a process where a dedicated circuit is shared by multiple users. Typically, data streams intersperse on a bit or byte basis (time division), or separate by different carrier frequencies (frequency division).

NonVolatile Random Access Memory (NVRAM)

Random Access Memory that retains its contents after electrical power turns off.

port

A physical interface that transmits and receives data.

port mirroring

A feature that sends received or transmitted traffic to a second destination.

port VLAN ID

Used to coordinate VLANs across multiple switches. When you create a port-based VLAN on a switch, assign a VLAN identification number (VLAN ID) and specify the ports that belong to the VLAN.

Power over Ethernet (PoE)

The capacity of a switch to power network devices, according to the 802.3af standard, over an Ethernet cable. Devices include IP phones, Wireless LAN Access Points (WLAN AP), security cameras, and access control points.

Protocol Data Units (PDUs)

A unit of data that is specified in a protocol of a specific layer and that consists of protocol-control information of the specific layer and possibly user data of that layer.

quality of service (QoS)

QoS features reserve resources in a congested network, allowing you to configure a higher priority to certain devices. For example, you can configure a higher priority to IP deskphones, which need a fixed bit rate, and, split the remaining bandwidth between data connections if calls in the network are more important than the file transfers.

Remote Network Monitoring (RMON)

Creates and displays alarms for user-defined events, gathers cumulative statistics for Ethernet interfaces, and tracks statistical history for Ethernet interfaces.

routing switch

Virtualizes the physical router interfaces to switches. A virtual router port, or interface, acts as a router port to consolidate switching and routing functions in the broadcast domain, or between broadcast domains, and enable IP routing for higher traffic volumes.

spanning tree

A simple, fully-connected active topology formed from the arbitrary physical topology of connected bridged Local Area Network components by relaying frames through selected bridge ports. The protocol parameters and states that are used and exchanged to facilitate the calculation of the active topology and to control the bridge relay function.

Spanning Tree Group (STG)

A collection of ports in one spanning tree instance.

Spanning Tree Protocol (STP)

MAC bridges use the STP to exchange information across Local Area Networks to compute the active topology of a bridged Local Area Network in accordance with the Spanning Tree Protocol algorithm.

stack

Stackable Avaya Ethernet Routing Switches can be connected in a stack configuration of two or more units, up to eight units maximum. A switch stack operates and is managed as a single virtual switch.

stand-alone

Refers to a single Avaya Ethernet Routing Switch operating outside a stack.

temporary base unit (TBU)

If an assigned base unit in a stack fails, the next unit in the stack automatically becomes the temporary base unit (TBU). The TBU maintains stack operations until the stack is restarted or the TBU fails. If the old base unit rejoins the stack, it does not take over from the TBU until the stack is reset.

time-to-live (TTL)

The field in a packet used to determine the valid duration for the packet. The TTL determines the packet lifetime. The system discards a packet with a TTL of zero.

Transmission Control Protocol (TCP)

Provides flow control and sequencing for transmitted data over an end-to-end connection.

trunk

A logical group of ports that behaves like a single large port.

type of service (TOS)

A field in the IPv4 header that determines the Class of Service prior to the standardization of Differentiated Services.

User Datagram Protocol (UDP)

In TCP/IP, a packet-level protocol built directly on the Internet Protocol layer. TCP/IP host systems use UDP for application-to-application programs.

Virtual Link Aggregation Control Protocol (VLACP)

Virtual Link Aggregation Control Protocol (VLACP) is a Layer 2 handshaking protocol that can detect end-to-end failure between two physical Ethernet interfaces.

Virtual Local Area Network (VLAN)

A Virtual Local Area Network is a group of hosts that communicate as if they are attached to the same broadcast domain regardless of their physical location. VLANs are layer 2 constructs.

Voice over IP (VOIP)

The technology that delivers voice information in digital form in discrete packets using the Internet Protocol (IP) rather than the traditional circuit-committed protocols of the public switched telephone network (PSTN).

wiring closet

A central termination area for telephone or network cabling or both.