Configuration — System Monitoring
Avaya Ethernet Routing Switch 4500
Series
Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

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

Licenses

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

Copyright

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

Third-party components

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.
Chapter 5: System diagnostics and statistics using ACLI................................. 35
  Navigation.................................................................................................................. 35
  Port statistics........................................................................................................... 35
    Viewing port-statistics.......................................................................................... 35
  Configuring Stack Monitor..................................................................................... 36
    Viewing the stack-monitor.................................................................................. 36
    Configuring the stack-monitor.......................................................................... 37
  Displaying stack health.......................................................................................... 38
  Viewing Stack Port Counters................................................................................ 39
  Clearing stack port counters................................................................................ 41
  Using the stack loopback test.............................................................................. 42
  Displaying port operational status....................................................................... 43
  Validating port operational status....................................................................... 43
  Showing port information..................................................................................... 44
  Viewing Environmental status using ACLI......................................................... 45

Chapter 6: RMON configuration using the ACLI.............................................. 47
  Navigation................................................................................................................ 47
  Viewing the RMON alarms.................................................................................... 47
  Viewing the RMON events.................................................................................... 48
  Viewing the RMON history................................................................................... 48
  Viewing the RMON statistics.............................................................................. 48
  Configuring RMON alarms.................................................................................. 48
  Deleting RMON alarms....................................................................................... 49
  Configuring RMON events settings..................................................................... 50
  Deleting RMON events settings......................................................................... 51
  Configuring RMON history settings................................................................. 51
  Deleting RMON history settings....................................................................... 52
  Configuring RMON statistics settings.............................................................. 52
  Deleting RMON statistics settings................................................................... 53

Chapter 7: IPFIX configuration using the ACLI.............................................. 55
  Navigation................................................................................................................ 55
  Global IPFIX management using ACLI............................................................... 55
    Enabling IPFIX globally using ACLI................................................................. 55
    Disabling IPFIX globally using ACLI............................................................... 56
    Viewing the global IPFIX status using ACLI..................................................... 56
  IPFIX flow management using ACLI.................................................................... 56
    Configuring the IPFIX aging interval using ACLI.............................................. 57
    Changing the IPFIX aging interval to default using ACLI.............................. 57
    Enabling the IPFIX exporter using ACLI.......................................................... 58
    Disabling the IPFIX exporter using ACLI........................................................ 58
    Configuring the IPFIX export interval using ACLI.......................................... 59
    Changing the IPFIX export interval to default using ACLI............................. 60
    Configuring the IPFIX refresh interval template using ACLI.......................... 60
    Changing the IPFIX refresh interval template to default using ACLI.............. 61
    Configuring the IPFIX refresh packets template using ACLI.......................... 61
    Changing the IPFIX refresh packets template to default using ACLI.............. 62
    Viewing IPFIX flow information using ACLI.................................................. 63
  IPFIX collector management using ACLI.......................................................... 64
    Enabling an IPFIX collector using ACLI.......................................................... 64
### Chapter 8: System diagnostics and statistics using Enterprise Device Manager

- **Navigation**
- **Prerequisites**
- **Configuring port mirroring using EDM**
- **Configuring Stack Monitor using EDM**
- **Viewing power supply information using EDM**
- **Viewing switch fan information using EDM**
- **Viewing switch temperature using EDM**
- **Chassis configuration statistics management using EDM**
- **Port configuration statistics management using EDM**
- **Viewing the IPFIX table using ACLI**
- **Disabling an IPFIX collector using ACLI**
- **Managing log information management using EDM**
- **Disabling an IPFIX collector using ACLI using EDM**
- **Viewing the IPFIX collector information using ACLI using EDM**
- **Port IPFIX management using ACLI**
- **Enabling port-based IPFIX for a stand-alone switch using ACLI**
- **Disabling port-based IPFIX for a stand-alone switch using ACLI**
- **Changing port-based IPFIX for a stand-alone switch to default using ACLI**
- **Viewing the port-based IPFIX status for a stand-alone switch using ACLI**
- **Enabling port-based IPFIX for a stack switch using ACLI**
- **Disabling port-based IPFIX for a stack switch using ACLI**
- **Changing port-based IPFIX for a stack switch to default using ACLI**
- **Viewing the port-based IPFIX status for a stack switch using ACLI**
- **Viewing the IPFIX table using ACLI**
- **Prerequisites**
- **Navigation**

### Chapter 9: RMON configuration using Enterprise Device Manager

- **Navigation**
- **Prerequisites**
- **RMON history management using EDM**
  - RMON history management using EDM navigation
  - Viewing RMON history using EDM
  - Creating RMON history characteristics using EDM
  - Disabling RMON history using EDM
  - Viewing RMON history statistics using EDM
  - RMON Ethernet statistics management using EDM
    - RMON Ethernet statistics management using EDM navigation
    - Viewing RMON Ethernet statistics using EDM
    - Enabling RMON Ethernet statistics gathering using EDM
    - Disabling RMON Ethernet statistics gathering using EDM
  - RMON alarm management using EDM
    - Alarm management using EDM navigation
    - Viewing RMON alarm configuration information using EDM
    - Creating an RMON alarm using EDM
    - Deleting an RMON alarm using EDM
  - Event management using EDM
    - Event management using EDM navigation
    - Viewing an event using EDM
    - Creating an event using EDM
    - Deleting an event using EDM
  - Managing log information management using EDM

### Chapter 10: Network monitoring configuration using Enterprise Device Manager

- **Navigation**

---

**Configuration — System Monitoring**

November 2010
Chapter 11: IPFIX configuration using Enterprise Device Manager

Navigation

Prerequisites

Configuring IPFIX globally using EDM

Configuring IPFIX flows using EDM

IPFIX collector management using EDM

IPFIX collector management using EDM navigation

Viewing IPFIX collectors using EDM

Configuring IPFIX collectors using EDM

Deleting IPFIX collectors using EDM

IPFIX port management using EDM

IPFIX port management using EDM navigation

Viewing IPFIX port information using EDM

Modifying specific IPFIX port configurations using EDM

Modifying all IPFIX port configurations using EDM

Graphing IPFIX exporter statistics for a collector using EDM

Viewing the IPFIX collector clear time using EDM
Chapter 1: New in this release

The following sections detail what is new in Avaya Ethernet Routing Switch 4500 Series Configuration — System Monitoring, NN47205-502 for Release 5.4.

- **Features** on page 7
- **Other changes** on page 8

**Features**

See the following sections for information about feature changes:

- **Enterprise Device Manager** on page 7
- **Dual Syslog Server Support** on page 7
- **IPFIX** on page 8

**Enterprise Device Manager**

Enterprise Device Manager (EDM) replaces both the Java-based Device Manager and Web-based management user interfaces. EDM is an embedded element management and configuration application for Avaya Ethernet Routing Switch 4500 Series switches. EDM provides a Web-based graphical user interface through a standard web browser for the convenience of full configuration and management on the switch, and retains the look and feel of Device Manager.

**Dual Syslog Server Support**

You can use the Dual Syslog Server Support feature to configure a second syslog server to run in tandem with the first. If you configure Dual Syslog Server Support, the system sends syslog messages simultaneously to both servers to ensure that syslog messages are logged, even if one of the servers becomes unavailable. For more information, see:

- **Viewing system logging information using ACLI** on page 26
- **Configuring remote system logging using ACLI** on page 31
- **Disabling remote system logging using ACLI** on page 32
- **Restoring remote system logging to default using ACLI** on page 33
New in this release

- Configuring remote system logging using EDM on page 123
- Viewing system logs using EDM on page 125

---

**IPFIX**

You can use IP Flow Information Export (IPFIX) to monitor traffic flows when you configure observation points to collect flow statistics over a designated time period. IPFIX is compatible with external IPFIX collectors like Avaya IP Flow Manager. For more information, see:

- IPFIX on page 20
- IPFIX configuration using ACLI on page 55
- IPFIX configuration using Enterprise Device Manager on page 129

---

**Other changes**

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

---

**Multiple Port Configuration**

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

For more information about EDM, see Avaya Ethernet Routing Switch 4500 Series Fundamentals, NN47205-102.
Chapter 2: Introduction

This document provides information you need to configure and use system monitoring for the Avaya Ethernet Routing Switch 4500 series Release 5.4.

Navigation

- System monitoring fundamentals on page 11
- Network monitoring configuration using ACLI on page 25
- Network monitoring configuration using Enterprise Device Manager on page 113
- System diagnostics and statistics using ACLI on page 35
- System diagnostics and statistics using Enterprise Device Manager on page 75
- RMON configuration using the ACLI on page 47
- RMON configuration using Enterprise Device Manager on page 95
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 4500 Series

The Avaya Ethernet Routing Switch 4500 Series displays diagnostic and operation information through the LEDs on the unit. Familiarize yourself with the interpretation of the LEDs on the 4500 series device. For detailed information regarding the interpretation of the LEDs, see Avaya Ethernet Routing Switch 4500 Series — Installation (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.

SNMP traps

SNMP traps are configured as notification controls. For more information about notification controls, see *Avaya Ethernet Routing Switch 4500 Series Configuration-Security* (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 14:

- %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
Table 1: IGMP syslog messages on page 14 describes the IGMP syslog messages and their severity.

Table 1: IGMP syslog messages

<table>
<thead>
<tr>
<th>Severity</th>
<th>Log Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informational</td>
<td>IGMP initialization success</td>
</tr>
<tr>
<td>Critical</td>
<td>IGMP initialization failed: Error code %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP policy initialized</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration loaded successfully</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration failed: Loaded to factory default</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration changed: Snooping enabled on VLAN %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration changed: Snooping disabled on VLAN %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration changed: Proxy enabled on VLAN %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration changed: Proxy disabled on VLAN %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration changed: Query time set to %d on VLAN %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration changed: Robust value set to %d on VLAN %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration changed: Version %d router port mask 0x%x set on VLAN %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration changed: Unknown multicast filter enabled</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration changed: Unknown multicast filter enabled</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration changed: Trunk %d created for IGMP</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration changed: Trunk %d removed for IGMP ports</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration changed: Mirror ports set</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration changed: Port %d added to VLAN %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP configuration changed: Port %d removed from VLAN %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP new Querier IP %x learned on port %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP exchange database sent by unit %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP exchange database received on unit %d from %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP exchange database done</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP stack join completed</td>
</tr>
<tr>
<td>Serious</td>
<td>IGMP not able to join stack: Error code %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP exchange group database sent by unit %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP exchange group database received on unit %d from %d</td>
</tr>
<tr>
<td>Informational</td>
<td>IGMP received report on VLAN %d for Group 0x%x on port %d</td>
</tr>
</tbody>
</table>
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 (LACPDUs) 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 4500 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** on page 16
- **External loopback test** on page 16

⚠️ **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 have been 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.

**Port mirroring**

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

**Note:**
When Port-Mirroring is enabled with one of the following modes Asrc, Adst, AsrcBdst, AsrcBdstOrBsrcAdst, AsrcOrAdst, XrxYtxOrYrxXtx, XrsYtx, higher available precedence will be used for all ports. Issuing "qos agent reset-default" will not free resources usec by Port Mirroring.

**Important:**
You must connect a probe device, such as the Avaya StackProbe or equivalent, to the designated monitor port to use this feature. Contact an Avaya sales agent for more information about the StackProbe.

**Important:**
When you have two units and remove or reboot one, port-mirroring does not print NONE on a standalone without a monitored or mirrored port. After a system reboot, the stack is completed and port-mirroring functions correctly.

**Port-based mirroring configuration**

The figure [Figure 1: Port-based mirroring example](#) on page 18 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.
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, 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 figure Figure 2: Address-based mirroring example on page 19 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).
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 two additional parameters:

- source port
- destination port

Beginning with Release 5.4, the Avaya Ethernet Routing Switch 4500 supports IPFIX through the creation and display of sampled information as well as the ability to export this sampled information.

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 Avaya Ethernet Routing Switch 4500 Series Configuration — Quality of Service, 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 4500 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.

![Diagram of alarm firing](image)

**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 Figure 4: Alarm example - threshold less than 260 on page 22). 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](image)

### 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 as an 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>
<thead>
<tr>
<th>Measurement</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSU1</td>
<td>Primary</td>
<td>If the power source is present and is the primary power source</td>
</tr>
<tr>
<td></td>
<td>Redundant</td>
<td>If the power source is present and is the redundant power source</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
<td>If the power source is missing or not providing power</td>
</tr>
<tr>
<td>Fan</td>
<td>OK</td>
<td>If the fan is working properly</td>
</tr>
<tr>
<td></td>
<td>FAIL</td>
<td>If any fan malfunction exists</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
<td>If the fan does not exist</td>
</tr>
<tr>
<td>Temperature</td>
<td>OK</td>
<td>If temperature is lower than 40C</td>
</tr>
<tr>
<td></td>
<td>HIGH</td>
<td>If temperature is greater than 40C</td>
</tr>
</tbody>
</table>
Chapter 4: Network monitoring configuration using ACLI

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

Navigation

- Viewing CPU utilization using ACLI on page 25
- Viewing memory utilization using ACLI on page 26
- Viewing system logging information using ACLI on page 26
- Configuring syslog capabilities using ACLI on page 28
- Configuring system logging using ACLI on page 29
- Disabling logging using ACLI on page 30
- Default logging using ACLI on page 30
- Clearing log messages using ACLI on page 30

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:
   
   \[ \text{show cpu-utilization} \]

Job Aid

The following figure is an example of CPU utilization output.
**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

<table>
<thead>
<tr>
<th>Unit</th>
<th>Total</th>
<th>Used</th>
<th>Free</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>128Mbytes</td>
<td>75Mbytes</td>
<td>53Mbytes</td>
</tr>
<tr>
<td>2</td>
<td>128Mbytes</td>
<td>75Mbytes</td>
<td>53Mbytes</td>
</tr>
</tbody>
</table>
```

**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

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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Displays local and remote system logging configuration status.</td>
</tr>
<tr>
<td>critical</td>
<td>Display critical log messages.</td>
</tr>
<tr>
<td>serious</td>
<td>Display serious log messages.</td>
</tr>
<tr>
<td>informational</td>
<td>Display informational log messages.</td>
</tr>
<tr>
<td>sort-reverse</td>
<td>Display informational log messages in reverse chronological order (beginning with most recent).</td>
</tr>
<tr>
<td>unit &lt;1-8&gt;</td>
<td>Display log messages for a specific switch in a stack.</td>
</tr>
</tbody>
</table>

**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.
ERS4500(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: 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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit &lt;1-8&gt;</td>
<td>all</td>
</tr>
</tbody>
</table>

Job Aid

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables or disables the event log (enabled is the default setting).</td>
</tr>
<tr>
<td>level critical</td>
<td>Specifies the level of logging stored in Dynamic Random Access Memory (DRAM).</td>
</tr>
<tr>
<td>nv-level critical</td>
<td>Specifies the level of logging stored in NVRAM.</td>
</tr>
<tr>
<td>remote</td>
<td>Configures remote logging parameters. Address: configure remote syslog address. Enable: enable remote logging. Level: configure remote logging level.</td>
</tr>
</tbody>
</table>
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.

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

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>]
```

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>]` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>address &lt;A.B.C.D</td>
<td>WORD&gt;</td>
</tr>
</tbody>
</table>
### Variable | Value
--- | ---
• 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.  

| 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  
• 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

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

```plaintext
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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Clears the primary remote system log server IP address.</td>
</tr>
<tr>
<td>secondary-address</td>
<td>Clears the secondary remote system log server IP address.</td>
</tr>
<tr>
<td>enable</td>
<td>Disables system message logging on the remote server.</td>
</tr>
<tr>
<td>level</td>
<td>Clears the remote server logging level.</td>
</tr>
</tbody>
</table>

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

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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Restores the primary remote system log server IP address to the factory default (0.0.0.0).</td>
</tr>
<tr>
<td>secondary-address</td>
<td>Restores the secondary remote system log server IP address to factory the default (0.0.0.0).</td>
</tr>
<tr>
<td>level</td>
<td>Restores the remote server logging level to the factory default (none).</td>
</tr>
</tbody>
</table>
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.

Navigation

- Port statistics on page 35
- Configuring Stack Monitor on page 36
- Displaying stack health on page 38
- Viewing Stack Port Counters on page 39
- Clearing stack port counters on page 41
- Clearing stack port counters on page 41
- Using the stack loopback test on page 42
- Displaying port operational status on page 43
- Validating port operational status on page 43
- Showing port information on page 44
- Viewing Environmental status using ACLI on page 45

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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>port &lt;portlist&gt;</code></td>
<td>The ports to display statistics for. When no port list is specified, all ports are shown.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables stack monitoring.</td>
</tr>
<tr>
<td>stack-size &lt;2-8&gt;</td>
<td>Sets the size of the stack to monitor. Valid range is from 2–8. By default the stack size is 2.</td>
</tr>
<tr>
<td>trap-interval &lt;30-300&gt;</td>
<td>Sets the interval between traps, in seconds. Valid range is from 30 to 300 seconds. By default the trap-interval is 60 seconds.</td>
</tr>
</tbody>
</table>

Setting default stack-monitor values

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

Configuring default stack monitor using ACLI

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

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.

<table>
<thead>
<tr>
<th>UNIT#</th>
<th>Switch Model</th>
<th>Cascade Up</th>
<th>Cascade Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (Base)</td>
<td>4526GTX</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>2</td>
<td>4526GTX-PWR</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>3</td>
<td>4524GT</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>4</td>
<td>4526T</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>5</td>
<td>4526T-PWR</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>6</td>
<td>4558GT-PWR</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>7</td>
<td>4550T</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>8</td>
<td>4526FX</td>
<td>OK</td>
<td>OK</td>
</tr>
</tbody>
</table>
```

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.
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).
```

<table>
<thead>
<tr>
<th>UNIT#</th>
<th>Switch Model</th>
<th>Cascade Up</th>
<th>Cascade Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (Base)</td>
<td>4526GTX</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>2</td>
<td>4526GTX-PWR</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>3</td>
<td>4524GT</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>4</td>
<td>4526T</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>6</td>
<td>4548GTX-PWR</td>
<td>LINK DOWN OR MISSING</td>
<td>OK</td>
</tr>
<tr>
<td>7</td>
<td>4550T</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>8</td>
<td>4526FX</td>
<td>OK</td>
<td>OK</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>UNIT#</th>
<th>Switch Model</th>
<th>Cascade Up</th>
<th>Cascade Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4526GTX</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>2 (Temporary Base)</td>
<td>4526GTX-PWR</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>3</td>
<td>4524GT</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>4</td>
<td>4526T</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>5</td>
<td>4526T-PWR</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>6</td>
<td>4548GTX-PWR</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>7</td>
<td>4550T</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>8</td>
<td>4526FX</td>
<td>OK</td>
<td>OK</td>
</tr>
</tbody>
</table>

---

**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

To show stacking statistics, enter the following command:

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

---

Variable Definitions

The following table describes the command parameters.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit &lt;1-8&gt;</td>
<td>Specifies the unit in the stack.</td>
</tr>
</tbody>
</table>

---

Job aid

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

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

<table>
<thead>
<tr>
<th>Transmitted</th>
<th>UP</th>
<th>DOWN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets</td>
<td>1257</td>
<td>1635</td>
</tr>
<tr>
<td>Multicasts</td>
<td>1246</td>
<td>1624</td>
</tr>
<tr>
<td>Broadcasts</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>Total Octets</td>
<td>407473</td>
<td>1765434</td>
</tr>
<tr>
<td>FCS Errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Undersized Packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Pause Frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Dropped On No Resources</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Clearing stack port counters**

Use the following procedure to clear the stack port counters

**Procedure Steps**

To clear stacking statistics, enter the following command:

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

**Variable Definitions**

The following table describes the command parameters.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit &lt;1-8&gt;</td>
<td>Specifies the unit in the stack.</td>
</tr>
</tbody>
</table>
Using the stack loopback test

Use this procedure to complete a stack loopback test

Configuring stack loopback test using ACLI

1. Access the Privileged Exec mode.
2. Enter the following command:
   ```
   stack loopback-test internal
   ```
3. Enter the following command:
   ```
   stack loopback-test external
   ```

Job aid

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

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

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

```
4524GT#stack loopback-test internal
  Testing uplink port ... ok
  Testing downlink port ... ok
  Internal 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#
```
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 4500 unit and on port 2 on another 4500 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

<table>
<thead>
<tr>
<th>Unit/Port</th>
<th>Filter Untagged Frames</th>
<th>Filter Unregistered Frames</th>
<th>PVID</th>
<th>PRI</th>
<th>Tagging</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>No</td>
<td>Yes</td>
<td>256</td>
<td>0</td>
<td>UntagAll</td>
<td>Unit 1, Port 1</td>
</tr>
<tr>
<td>1/2</td>
<td>No</td>
<td>Yes</td>
<td>2</td>
<td>0</td>
<td>UntagAll</td>
<td>Unit 1, Port 2</td>
</tr>
</tbody>
</table>

Table 4: VLAN ID port member configuration

<table>
<thead>
<tr>
<th>Unit/Port</th>
<th>VLAN</th>
<th>VLAN Name</th>
<th>VLAN</th>
<th>VLAN Name</th>
<th>VLAN</th>
<th>VLAN Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>256</td>
<td>VLAN #256</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/2</td>
<td>2</td>
<td>VLAN-2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5: Spanning-tree port configurations

<table>
<thead>
<tr>
<th>Unit</th>
<th>Port</th>
<th>Trunk</th>
<th>Participation</th>
<th>Priority</th>
<th>Path</th>
<th>Cost</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td></td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td></td>
<td>Normal</td>
<td>Learning</td>
<td>128</td>
<td>20000</td>
<td>Forwarding</td>
</tr>
</tbody>
</table>

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 is an example of the output of the show environmental command.

```
4548GT-PWR>enable
4548GT-PWR#show environmental

<table>
<thead>
<tr>
<th>Unit#</th>
<th>PSU1</th>
<th>PSU2</th>
<th>FAN1</th>
<th>FAN2</th>
<th>FAN3</th>
<th>FAN4</th>
<th>Temperature</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Primary</td>
<td>N/A</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK 33C</td>
</tr>
<tr>
<td>2</td>
<td>Primary</td>
<td>N/A</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>HIGH 41C</td>
</tr>
</tbody>
</table>

4548GT-PWR#
```
Chapter 6: RMON configuration using the ACLI

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

Navigation

- Viewing the RMON alarms on page 47
- Viewing the RMON events on page 48
- Viewing the RMON history on page 48
- Viewing the RMON statistics on page 48
- Configuring RMON alarms on page 48
- Deleting RMON alarms on page 49
- Configuring RMON events settings on page 50
- Deleting RMON events settings on page 51
- Configuring RMON history settings on page 51
- Deleting RMON history settings on page 52
- Configuring RMON statistics settings on page 52
- Deleting RMON statistics settings on page 53

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:

   ```
   mon 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.

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

Deleting RMON alarms

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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-65535</td>
<td>Unique index for the event entry.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Unique index for the event entry.</td>
</tr>
<tr>
<td>[log]</td>
<td>Records events in the log table.</td>
</tr>
<tr>
<td>[trap]</td>
<td>Generates SNMP trap messages for events.</td>
</tr>
<tr>
<td>[description &lt;LINE&gt;]</td>
<td>Specifies a textual description for the event.</td>
</tr>
</tbody>
</table>
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:
   ```plaintext
   no rmon alarm [1-65535]
   ```

Variable Definitions

The following table describes the command parameters.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-65535</td>
<td>Unique index for the event entry.</td>
</tr>
</tbody>
</table>

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:
   ```plaintext
   rmon history <1-65535> <LINE> <1-65535> <1-3600> [owner <LINE>]
   ```
Variable Definitions

The following table describes the command parameters.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Unique index for the history entry.</td>
</tr>
<tr>
<td>&lt;LINE&gt;</td>
<td>Specifies the port number to be monitored.</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>The number of history buckets (records) to keep.</td>
</tr>
<tr>
<td>&lt;1-3600&gt;</td>
<td>The sampling rate (how often a history sample is collected).</td>
</tr>
<tr>
<td>[owner &lt;LINE&gt;]</td>
<td>Specifies an owner string to identify the history entry.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-65535</td>
<td>Unique index for the event entry.</td>
</tr>
</tbody>
</table>

Configuring RMON statistics settings

Use this procedure to configure RMON statistics settings.
Configuring RMON statistics settings using ACLI

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.

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

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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-65535</td>
<td>Unique index for the event entry.</td>
</tr>
</tbody>
</table>
RMON configuration using the ACLI
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).

Navigation

- Global IPFIX management using ACLI on page 55
- IPFIX flow management using ACLI on page 56
- IPFIX collector management using ACLI on page 64
- Port IPFIX management using ACLI on page 67
- Viewing the IPFIX table using ACLI on page 73

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

To enable IPFIX globally, enter the following command:
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

To enable IPFIX globally, enter 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

To display the global IPFIX operational status, 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

To configure the IPFIX aging interval, 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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>aging-interval &lt;0-2147400&gt;</td>
<td>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 have been updated. If no new updates are found between two checks, the system deletes the records.</td>
</tr>
<tr>
<td>slot &lt;unit_number&gt;</td>
<td>Specifies whether the switch is a standalone or part of a stack. A value of 1 indicates a standalone switch.</td>
</tr>
</tbody>
</table>

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

To change the IPFIX aging interval to default, 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

To enable the IPFIX exporter, enter one of the following commands:

• 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.

• default ip ipfix exporter-enable
Prerequisites

Log on to the Global Configuration mode in ACLI.

Procedure steps

To disable the IPFIX exporter, 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

To configure the IPFIX export interval, 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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>export-interval &lt;10-3600&gt;</td>
<td>Specifies the frequency of data exports to the collector in seconds. Values range from 10 to 3600 seconds. The default is 50 seconds.</td>
</tr>
</tbody>
</table>
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

To change the IPFIX export interval to default, 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

To configure the IPFIX refresh interval template, 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.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>template-refresh-interval</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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

To change the IPFIX template refresh interval to default, 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

To configure the IPFIX refresh packets template, 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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>template-refresh-packets &lt;10000-100000&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

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

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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot &lt;unit_number&gt;</td>
<td>Displays information for a switch that is a standalone or part of a stack. A value of 1 indicates a standalone switch.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aging Interval (sec)</td>
<td>Indicates the aging interval of the flow record in seconds. Values range from 0–2147400 seconds. The default is 30 seconds.</td>
</tr>
<tr>
<td>Active Timeout (min)</td>
<td>Indicates the flow record active timeout value in minutes. This is not a configurable value.</td>
</tr>
</tbody>
</table>
## IPFIX configuration using ACLI

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 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 on to the Global Configuration mode in ACLI.

Procedure steps

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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;A.B.C.D&gt;</td>
<td>Specifies the IPFIX collector IP address.</td>
</tr>
</tbody>
</table>

Disabling an IPFIX collector using ACLI

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

Prerequisites

Log on to the Global Configuration mode in ACLI.

Procedure steps

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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;A.B.C.D&gt;</td>
<td>Specifies the IPFIX collector IP address.</td>
</tr>
</tbody>
</table>

Viewing the IPFIX collector information using ACLI

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

Prerequisites

Log on to the User EXEC mode in ACLI.

Procedure steps

1. To view information for all configured IPFIX collectors enter the following command:
   ```bash
   show ip ipfix collector
   ```
2. To view information for a specific configured IPFIX collector, enter the following command:
   ```bash
   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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;A.B.C.D&gt;</td>
<td>Displays the operational status for a specific IPFIX collector IP address.</td>
</tr>
</tbody>
</table>
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 on 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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>port &lt;port_list&gt;</td>
<td>Specifies an individual port or list of ports.</td>
</tr>
</tbody>
</table>

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 on to the Interface Configuration mode in ACLI.

Procedure steps

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

```plaintext
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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Disables IPFIX for the selected port or ports.</td>
</tr>
<tr>
<td>port &lt;port_list&gt; enable</td>
<td>Disables IPFIX for an alternate individual port or list of ports.</td>
</tr>
</tbody>
</table>

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 on 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:

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

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

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Changes the IPFIX operational status for the selected port or ports to default.</td>
</tr>
<tr>
<td>port &lt;port_list&gt; enable</td>
<td>Changes the IPFIX operational status for a port or list of ports to default.</td>
</tr>
</tbody>
</table>

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 on 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.
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 on to the Interface Configuration mode in ACLI.

Procedure steps

1. To enable IPFIX for the selected port or ports, enter the following command:
   
   \[ \text{ip ipfix enable} \]

2. To enable IPFIX for alternate ports, enter the following command:
   
   \[ \text{ip ipfix port <unit_number/port_list> enable} \]

Variable definitions

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port_list&gt;</td>
<td>Specifies a specific port or list of ports for which to display the IPFIX operational mode for to default.</td>
</tr>
</tbody>
</table>

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 on 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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>port &lt;unit_number/port_list&gt;</td>
<td>Specifies a switch number in the stack and an individual port or list of ports.</td>
</tr>
</tbody>
</table>

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 on 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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>port &lt;unit_number/port_list&gt;</td>
<td>Specifies a switch number in the stack and an individual port or list of ports.</td>
</tr>
</tbody>
</table>

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 on to the User EXEC mode in ACLI.

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.
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 on to the User EXEC mode in ACLI.

Procedure steps

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

The following table defines parameters that you enter with the `show ip ipfix table <unit_number> [sort-by <sort_rule>] [sort-order <sort_order>] [display <num_entries>]` command.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;unit_number/port_list&gt;</code></td>
<td>Specifies a switch number in the stack and an individual port or list of ports.</td>
</tr>
<tr>
<td><code>display &lt;num_entries&gt;</code></td>
<td>Specifies the number of entries to display. Values include:</td>
</tr>
<tr>
<td></td>
<td>• all—displays all available entries</td>
</tr>
<tr>
<td></td>
<td>• top-10—displays first 10 entries</td>
</tr>
<tr>
<td></td>
<td>• top-25—displays first 25 entries</td>
</tr>
<tr>
<td></td>
<td>• top-50—displays first 50 entries</td>
</tr>
<tr>
<td></td>
<td>• top-100—displays first 100 entries</td>
</tr>
<tr>
<td></td>
<td>• top-200—displays first 200 entries</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>sort-by &lt;sort_rule&gt;</td>
<td>Specifies a rule to sort data by. Values include:</td>
</tr>
<tr>
<td></td>
<td>• byte-count—data byte number</td>
</tr>
<tr>
<td></td>
<td>• dest-addr—destination IP address</td>
</tr>
<tr>
<td></td>
<td>• first-pkt-time—first packet time</td>
</tr>
<tr>
<td></td>
<td>• last-pkt-time—last packet time</td>
</tr>
<tr>
<td></td>
<td>• pkt-count—packet number</td>
</tr>
<tr>
<td></td>
<td>• port—port number</td>
</tr>
<tr>
<td></td>
<td>• protocol—protocol number</td>
</tr>
<tr>
<td></td>
<td>• source-addr—source IP address</td>
</tr>
<tr>
<td></td>
<td>• TCP-UDP-dest-port—TCP/UDP destination port</td>
</tr>
<tr>
<td></td>
<td>• TCP-UDP-src-port—TCP/UDP source port</td>
</tr>
<tr>
<td></td>
<td>• TOS—type of service</td>
</tr>
<tr>
<td>sort-order &lt;sort_order&gt;</td>
<td>Specifies the order in which to sort data. Values include:</td>
</tr>
<tr>
<td></td>
<td>• ascending</td>
</tr>
<tr>
<td></td>
<td>• descending</td>
</tr>
<tr>
<td>&lt;unit_number&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>
Chapter 8: System diagnostics and statistics using Enterprise Device Manager

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

Navigation

• Configuring port mirroring using EDM on page 75
• Configuring Stack Monitor using EDM on page 77
• Viewing power supply information using EDM on page 78
• Viewing switch fan information using EDM on page 79
• Viewing switch temperature using EDM on page 79
• Chassis configuration statistics management using EDM on page 80
• Port configuration statistics management using EDM on page 87

Prerequisites

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

Configuring port mirroring using EDM

Use the following procedure to configure port mirroring using EDM.
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. On the toolbar, click **Insert**.
   The Insert Port Mirrors dialog box appears.
5. Configure the parameters as required.
6. Click **Insert**.

Variable definitions

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Numerical assignment of the port mirroring.</td>
</tr>
<tr>
<td>Port Mode</td>
<td>The port monitoring mode. The following options are available:</td>
</tr>
<tr>
<td></td>
<td>• Adst</td>
</tr>
<tr>
<td></td>
<td>• Asrc</td>
</tr>
<tr>
<td></td>
<td>• AsrcBdst</td>
</tr>
<tr>
<td></td>
<td>• AsrcBdstorBsorcAdst</td>
</tr>
<tr>
<td></td>
<td>• AsrcorAdst</td>
</tr>
<tr>
<td></td>
<td>• manytoOneRx</td>
</tr>
<tr>
<td></td>
<td>• manytoOneRxTx</td>
</tr>
<tr>
<td></td>
<td>• manytoOneTx</td>
</tr>
<tr>
<td></td>
<td>• Xrx</td>
</tr>
<tr>
<td></td>
<td>• XrxorXtx</td>
</tr>
<tr>
<td></td>
<td>• XrxorYtx</td>
</tr>
<tr>
<td></td>
<td>• Xrxytx</td>
</tr>
<tr>
<td></td>
<td>• XrxytxorYrxXtx</td>
</tr>
<tr>
<td></td>
<td>• Xtx</td>
</tr>
<tr>
<td></td>
<td>The default value is Adst.</td>
</tr>
</tbody>
</table>
Variable | Value
--- | ---
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.
MacAddressA | MAC address of the monitored port using Sarc/Adst related mode.
MacAddressB | MAC address of the monitored port using Bsrc/Bdst related mode.
Allow traffic | Allows or disallow traffic.

### 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. On the toolbar, click **Apply**.

### Variable definitions

The following table describes the Stack Monitor tab fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>StackErrorNotificationEnabled</td>
<td>Enables or disables the Stack Monitoring feature.</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit 1 Primary Power Supply</td>
<td>Indicates the status of primary power supply.</td>
</tr>
<tr>
<td>Unit 1 Redundant Power Supply</td>
<td>Indicates the status of redundant power supply.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit 1 Fan 1</td>
<td>Indicates the status of Fan 1.</td>
</tr>
<tr>
<td>Unit 1 Fan 2</td>
<td>Indicates the status of Fan 2.</td>
</tr>
<tr>
<td>Unit 1 Fan 3</td>
<td>Indicates the status of Fan 3.</td>
</tr>
<tr>
<td>Unit 1 Fan 4</td>
<td>Indicates the status of Fan 4.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit</td>
<td>Indicates the switch unit number in a stack. For a standalone switch, the default value is 1.</td>
</tr>
<tr>
<td>Temperature</td>
<td>Indicates the switch unit operating temperature.</td>
</tr>
</tbody>
</table>

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.
Variable definitions

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

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

**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.

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

**Graphing chassis ICMP Out statistics using EDM**

Use this procedure to display and graph ICMP Out statistics.

**Related topics:**
- Procedure steps on page 83
- Variable definitions on page 84

**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.

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

### 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.

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

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

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

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

---

**Graphing port RMON statistics using EDM**

Use this procedure to display and graph RMON Ethernet statistics.

**Related topics:**
- [Procedure steps](#) on page 91
- [Variable definitions](#) on page 92

**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.

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

---

**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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NoResourcesPktsDropped</td>
<td>The number of packets dropped due to switch memory shortage.</td>
</tr>
</tbody>
</table>
Chapter 9: 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).

Navigation

- Viewing RMON history using EDM on page 96
- Disabling RMON history using EDM on page 99
- Viewing RMON history statistics using EDM on page 99
- Enabling RMON Ethernet statistics gathering using EDM on page 103
- Disabling RMON Ethernet statistics gathering using EDM on page 104
- RMON alarm management using EDM on page 104
- Event management using EDM on page 108
- Managing log information management using EDM on page 111

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.
RMON history management using EDM navigation

- Viewing RMON history using EDM on page 96
- Creating RMON history characteristics using EDM on page 97
- Disabling RMON history using EDM on page 99

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 following:

- 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.

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

**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.

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SampleIndex</td>
<td>The sample number. As history samples are taken, they are assigned greater sample numbers.</td>
</tr>
<tr>
<td>Utilization</td>
<td>Estimate the percentage of the capacity of a link that is used during the sampling interval.</td>
</tr>
<tr>
<td>Octets</td>
<td>The number of octets received on the link during the sampling period.</td>
</tr>
<tr>
<td>Pkts</td>
<td>The number of packets received on the link during the sampling period.</td>
</tr>
<tr>
<td>BroadcastPkts</td>
<td>The number of packets received on the link during the sampling interval that destined for the packet address.</td>
</tr>
<tr>
<td>MulticastPkts</td>
<td>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.</td>
</tr>
<tr>
<td>DropEvents</td>
<td>The number of received packets that are dropped because of system resource constraints.</td>
</tr>
<tr>
<td>CRCAlignErrors</td>
<td>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).</td>
</tr>
<tr>
<td>UndersizePkts</td>
<td>The number of packets received during the sampling interval are less than 64 octets long (including FCS octets, but not framing bits).</td>
</tr>
<tr>
<td>OversizePkts</td>
<td>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).</td>
</tr>
<tr>
<td>Fragments</td>
<td>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 octets (FCS Error) or a nonintegral number of octets (Alignment Error).</td>
</tr>
<tr>
<td>Collisions</td>
<td>The best estimate of the number of collisions on an Ethernet segment during a sampling interval.</td>
</tr>
</tbody>
</table>
**RMON Ethernet statistics management using EDM**

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

**RMON Ethernet statistics management using EDM navigation**

- Viewing RMON Ethernet statistics using EDM on page 101
- Enabling RMON Ethernet statistics gathering using EDM on page 103
- Disabling RMON Ethernet statistics gathering using EDM on page 104

**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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>A unique value assigned to each interface. An index identifies an entry in a table.</td>
</tr>
<tr>
<td>Port</td>
<td>A port on the device.</td>
</tr>
<tr>
<td>DropEvents</td>
<td>The number of received packets that are dropped because of system resource constraints.</td>
</tr>
<tr>
<td>Octets</td>
<td>The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable</td>
</tr>
</tbody>
</table>


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

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>128 ..255</td>
<td>The total number of packets (including bad packets) received that are greater than 127 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>256..511</td>
<td>The total number of packets (including bad packets) received that are greater than 255 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>512..1023</td>
<td>The total number of packets (including bad packets) received that are greater than 511 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>1024..1518</td>
<td>The total number of packets (including bad packets) received that are greater than 1023 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Owner</td>
<td>The network management system that created this entry.</td>
</tr>
</tbody>
</table>

---

### 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**.

---

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

Alarm management using EDM navigation

- Viewing RMON alarm configuration information using EDM on page 105
- Creating an RMON alarm using EDM on page 106
- Deleting an RMON alarm using EDM on page 108

Prerequisites

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

---

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device. Range is 1–65535.</td>
</tr>
<tr>
<td>Interval</td>
<td>Time period (in seconds) over which the data is sampled and compared with the rising and falling thresholds.</td>
</tr>
<tr>
<td>Variable Name</td>
<td>Name and type of alarm—indicated by the format:</td>
</tr>
<tr>
<td></td>
<td>• alarmname.x where x=0 indicates a chassis alarm.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• alarmname with no dot or index is a port-related alarm and displays in the port selection tool.</td>
</tr>
<tr>
<td>Sample Type</td>
<td>Specifies the sample type—absolute or delta.</td>
</tr>
<tr>
<td>Value</td>
<td>Indicates the value of the alarm statistic during the last sampling period, compared with the rising and falling thresholds.</td>
</tr>
<tr>
<td>StartupAlarm</td>
<td>Indicates the type of alarm generated at startup, based on rising and falling thresholds. Values include:</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>risingAlarm</td>
<td></td>
</tr>
<tr>
<td>risingOrFallingAlarm</td>
<td></td>
</tr>
<tr>
<td>fallingAlarm</td>
<td></td>
</tr>
<tr>
<td>RisingThreshold</td>
<td>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.</td>
</tr>
<tr>
<td>RisingEventIndex</td>
<td>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.)</td>
</tr>
<tr>
<td>FallingThreshold</td>
<td>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.</td>
</tr>
<tr>
<td>FallingEventIndex</td>
<td>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.)</td>
</tr>
<tr>
<td>Owner</td>
<td>Specifies the owner name.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates the status of the alarm entry.</td>
</tr>
</tbody>
</table>

---

### 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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variable</td>
<td>Name and type of alarm—indicated by the format:</td>
</tr>
<tr>
<td></td>
<td>• alarmname.x where x=0 indicates a chassis alarm.</td>
</tr>
<tr>
<td></td>
<td>• alarmname. where you must specify the index. This is a card</td>
</tr>
<tr>
<td></td>
<td>number for module-related alarms, an STG ID for spanning</td>
</tr>
<tr>
<td></td>
<td>tree group alarms (the default STG is 1, other STG IDs are</td>
</tr>
<tr>
<td></td>
<td>user-configured), or the Ether Statistics Control Index for</td>
</tr>
<tr>
<td></td>
<td>RMON Stats alarms.</td>
</tr>
<tr>
<td></td>
<td>• alarmname with no dot or index is a port-related alarm and</td>
</tr>
<tr>
<td></td>
<td>displays in the port selection tool.</td>
</tr>
<tr>
<td>Sample Type</td>
<td>Specifies the sample type—absolute or delta.</td>
</tr>
<tr>
<td>Interval</td>
<td>Specifies the time period (in seconds) over which the data is</td>
</tr>
<tr>
<td></td>
<td>sampled and compared with the rising and falling thresholds.</td>
</tr>
<tr>
<td>Index</td>
<td>Uniquely identifies an entry in the alarm table. Each such entry</td>
</tr>
<tr>
<td></td>
<td>defines a diagnostic sample at a particular interval for an object</td>
</tr>
<tr>
<td></td>
<td>on the device. Range is 1–65535.</td>
</tr>
<tr>
<td>RisingThreshold</td>
<td>When the current sampled value is greater than or equal to this</td>
</tr>
<tr>
<td></td>
<td>threshold, and the value at the last sampling interval is less</td>
</tr>
<tr>
<td></td>
<td>than this threshold, generates a single event.</td>
</tr>
<tr>
<td>RisingEventIndex</td>
<td>Specifies the index of the event entry that is used when a rising</td>
</tr>
<tr>
<td></td>
<td>threshold is crossed. The event entry identified by a particular</td>
</tr>
<tr>
<td></td>
<td>value of this index is the same as identified by the same value of</td>
</tr>
<tr>
<td></td>
<td>the event index object. (Generally, accept the default that is</td>
</tr>
<tr>
<td></td>
<td>already filled in.)</td>
</tr>
<tr>
<td>FallingThreshold</td>
<td>When the current sampled value is less than or equal to this</td>
</tr>
<tr>
<td></td>
<td>threshold, and the value at the last sampling interval is greater</td>
</tr>
<tr>
<td></td>
<td>than this threshold, generates a single event.</td>
</tr>
<tr>
<td>FallingEventIndex specifies the</td>
<td>Specifies the index of the event entry that is used when a falling</td>
</tr>
<tr>
<td></td>
<td>threshold is crossed. The event entry identified by a particular</td>
</tr>
<tr>
<td></td>
<td>value of this index is the same as identified by the same value of</td>
</tr>
<tr>
<td></td>
<td>the event index object. (Generally, accept the default that is</td>
</tr>
<tr>
<td></td>
<td>already filled in.)</td>
</tr>
<tr>
<td>Owner</td>
<td>Specifies the owner name.</td>
</tr>
</tbody>
</table>
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.

Event management using EDM navigation

- Viewing an event using EDM on page 109
- Creating an event using EDM on page 110
- Deleting an event using EDM on page 110

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>This index uniquely identifies an entry in the event table. Each entry defines one event that is to be generated when the appropriate conditions occur.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies whether the event is a rising or falling event.</td>
</tr>
</tbody>
</table>
| 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.

Variable definitions

The following table describes the Log tab fields.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Specifies when an event occurs that activates the log entry.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies whether the event is a rising or falling event.</td>
</tr>
<tr>
<td>EventIndex</td>
<td>Specifies the event index.</td>
</tr>
</tbody>
</table>

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.

Prerequisites

- Open one of the supported browsers.
- Enter the IP address of the switch to open an EDM session.
Chapter 10: Network monitoring configuration using Enterprise Device Manager

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

Navigation

- Viewing CPU and memory utilization using EDM on page 113
- Switch stack information management using EDM on page 115
- Viewing stack health using EDM on page 120
- Configuring the system log using EDM on page 121
- Configuring remote system logging using EDM on page 123
- Viewing system logs using EDM on page 125
- EDM MIB Web page on page 126

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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit</td>
<td>Indicates the numerical representation of the unit.</td>
</tr>
<tr>
<td>Last10Seconds</td>
<td>Indicates the CPU usage, in percentage, for the last 10 seconds.</td>
</tr>
<tr>
<td>Last1Minute</td>
<td>Indicates the CPU usage, in percentage, for the last minute.</td>
</tr>
<tr>
<td>Last10Minutes</td>
<td>Indicates the CPU usage, in percentage, for the last 10 minutes.</td>
</tr>
<tr>
<td>Last1Hour</td>
<td>Indicates the CPU usage, in percentage, for the last hour.</td>
</tr>
<tr>
<td>Last24Hours</td>
<td>Indicates the CPU usage, in percentage, for the last 24 hours.</td>
</tr>
<tr>
<td>TotalCPUUsage</td>
<td>Indicates the CPU usage in percentage, since system start up.</td>
</tr>
<tr>
<td>MemoryTotalMB</td>
<td>Indicates the total memory present, in megabytes, on the unit.</td>
</tr>
<tr>
<td>MemoryAvailableMB</td>
<td>Indicates the memory remaining available on the unit.</td>
</tr>
<tr>
<td>MemoryUsedMB</td>
<td>Indicates the memory being used on the unit.</td>
</tr>
</tbody>
</table>
Switch stack information management using EDM

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

Switch stack information management using EDM navigation

- Viewing stack information using EDM on page 115
- Editing stack information using EDM on page 117
- Viewing pluggable ports using EDM on page 119

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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indx</td>
<td>Indicates the line number for stack info.</td>
</tr>
<tr>
<td>Descr</td>
<td>Describes the component or subcomponent. If not available, the value is a zero length string.</td>
</tr>
<tr>
<td>Location</td>
<td>Indicates the geographic location of a component in a system modeled as a chassis, but possibly physically implemented with geographically separate devices</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td></td>
<td>connected to exchange management information. Chassis modeled in this manner are sometimes referred to as virtual chassis. An example value is: 4th flr wiring closet in blg A.</td>
</tr>
<tr>
<td><strong>Important:</strong></td>
<td>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.</td>
</tr>
<tr>
<td>LstChng</td>
<td>Indicates the value of sysUpTime when it was detected that the component or sub-component was added to the chassis. If this action has not occurred since the cold or warm start of the agent, the value is zero.</td>
</tr>
<tr>
<td>AdminState</td>
<td>Indicates the state of the component or subcomponent.</td>
</tr>
<tr>
<td></td>
<td>• enable: enables operation</td>
</tr>
<tr>
<td></td>
<td>• reset: resets component</td>
</tr>
<tr>
<td>OperState</td>
<td>Indicates the current operational state of the component. The possible values are</td>
</tr>
<tr>
<td></td>
<td>• other: another state</td>
</tr>
<tr>
<td></td>
<td>• notAvail: state not available</td>
</tr>
<tr>
<td></td>
<td>• removed: component removed</td>
</tr>
<tr>
<td></td>
<td>• disabled: operation disabled</td>
</tr>
<tr>
<td></td>
<td>• normal: normal operation</td>
</tr>
<tr>
<td></td>
<td>• resetInProg: reset in progress</td>
</tr>
<tr>
<td></td>
<td>• testing: performing a self test</td>
</tr>
<tr>
<td></td>
<td>• warning: operating at warning level</td>
</tr>
<tr>
<td></td>
<td>• nonFatalErr: operating at error level</td>
</tr>
<tr>
<td></td>
<td>• fatalErr: error stopped operation</td>
</tr>
<tr>
<td>Ver</td>
<td>Indicates the version number of the component or subcomponent. If not available, the value is a zero-length string.</td>
</tr>
</tbody>
</table>
Variable | Value
--- | ---
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.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indx</td>
<td>Indicates the line number for stack info. This is a read-only cell.</td>
</tr>
<tr>
<td>Descr</td>
<td>Describes the component or subcomponent. If not available, the value is a zero length string. This is a read-only cell.</td>
</tr>
<tr>
<td>Location</td>
<td>Specifies the geographic location of a component in a system modeled as a chassis, but possibly physically implemented with geographically separate devices connected to exchange management information. Chassis modeled in this manner are sometimes referred to as virtual chassis. An example value is: 4th flr wiring closet in blg A. <strong>Important:</strong> 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.</td>
</tr>
<tr>
<td>LstChng</td>
<td>Indicates the value of sysUpTime when it was detected that the component or subcomponent 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.</td>
</tr>
</tbody>
</table>
| 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 |
### 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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit</td>
<td>Identifies the unit number.</td>
</tr>
<tr>
<td>Port</td>
<td>Identifies the number of the pluggable port.</td>
</tr>
<tr>
<td>PortType</td>
<td>Identifies the type of the pluggable port.</td>
</tr>
<tr>
<td>VendorName</td>
<td>Identifies the vendor's name.</td>
</tr>
<tr>
<td>VendorOUI</td>
<td>Identifies the Vendor Organizationally Unique Identifier</td>
</tr>
<tr>
<td>VendorPartNo</td>
<td>Identifies the vendor's part number.</td>
</tr>
<tr>
<td>VendorRevision</td>
<td>Identifies the vendor's revision.</td>
</tr>
<tr>
<td>VendorSerial</td>
<td>Identifies the vendor's serial number.</td>
</tr>
<tr>
<td>HWOptions</td>
<td>Identifies the hardware options.</td>
</tr>
<tr>
<td>DateCode</td>
<td>Identifies the date code.</td>
</tr>
<tr>
<td>VendorData</td>
<td>Identifies vendor data.</td>
</tr>
<tr>
<td>OrderCode</td>
<td>Identifies the order code.</td>
</tr>
</tbody>
</table>

---

**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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Units Found</td>
<td>Indicates the number of switch units in the stack.</td>
</tr>
<tr>
<td>Stack Health Check</td>
<td>Indicates the stack health.</td>
</tr>
<tr>
<td>Stack Diagnosis</td>
<td>Indicates the stack mode.</td>
</tr>
<tr>
<td>Unit</td>
<td>Indicates the unit number.</td>
</tr>
<tr>
<td>Description</td>
<td>Describes each unit in the stack.</td>
</tr>
<tr>
<td>Cascade Up</td>
<td>Indicates the cascade up link status.</td>
</tr>
<tr>
<td>Cascade Down</td>
<td>Indicates the cascade down link status.</td>
</tr>
<tr>
<td>Stack Role</td>
<td>Indicates which unit is the base unit.</td>
</tr>
</tbody>
</table>

---

### 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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Enables (on) or disables (off) the system log.</td>
</tr>
<tr>
<td>BufferFullAction</td>
<td>Specifies the action for the system to take when the buffer space allocated for system log messages is exhausted.</td>
</tr>
<tr>
<td></td>
<td>• overwrite—previously logged messages are overwritten</td>
</tr>
<tr>
<td></td>
<td>• 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).</td>
</tr>
<tr>
<td>Volatile - CurSize</td>
<td>Indicates the number of messages currently stored in volatile memory.</td>
</tr>
<tr>
<td>Volatile - SaveTargets</td>
<td>Specifies the type of system messages to save in volatile memory.</td>
</tr>
<tr>
<td></td>
<td>• critical—only messages classified as critical are saved in volatile memory</td>
</tr>
<tr>
<td></td>
<td>• critical/serious—only messages classified as critical and serious are saved in volatile memory</td>
</tr>
<tr>
<td></td>
<td>• critical/serious/inform—only messages classified as critical, serious, and informational are saved in volatile memory</td>
</tr>
<tr>
<td></td>
<td>• none—no system log messages are saved in volatile memory</td>
</tr>
<tr>
<td>Variable</td>
<td>Value</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>non-Volatile - CurSize</td>
<td>Indicates the number of messages currently stored in non-volatile memory.</td>
</tr>
<tr>
<td>non-Volatile - SaveTargets</td>
<td>Specifies the type of system messages to save in non-volatile memory.</td>
</tr>
<tr>
<td></td>
<td>• critical—only messages classified as critical are saved in volatile memory</td>
</tr>
<tr>
<td></td>
<td>• critical/serious—only messages classified as critical and serious are saved in non-volatile memory</td>
</tr>
<tr>
<td></td>
<td>• critical/serious/inform—only messages classified as critical, serious, and informational are saved in non-volatile memory</td>
</tr>
<tr>
<td></td>
<td>• none—no system log messages are saved in volatile memory</td>
</tr>
<tr>
<td>ClearMessageBuffers</td>
<td>Specifies the types system log messages to delete from volatile and non-volatile memory.</td>
</tr>
<tr>
<td></td>
<td>• volCritical—only messages classified as critical are deleted from volatile memory</td>
</tr>
<tr>
<td></td>
<td>• volSerious—only messages classified as serious are deleted from volatile memory</td>
</tr>
<tr>
<td></td>
<td>• volInformational—only messages classified as informational are deleted from volatile memory</td>
</tr>
<tr>
<td></td>
<td>• nonVolCritical—only messages classified as critical are deleted from non-volatile memory</td>
</tr>
<tr>
<td></td>
<td>• nonVolSerious—only messages classified as serious are deleted from non-volatile memory</td>
</tr>
</tbody>
</table>

### 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. On the tool bar, click Apply.

Variable definitions

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RemoteSyslogAddressType</td>
<td>Specifies the type of IP address of the remote system log server.</td>
</tr>
<tr>
<td>RemoteSyslogAddress</td>
<td>Specifies the IP address of the remote system log server to send system log messages to.</td>
</tr>
<tr>
<td>SecondarySyslogAddressType</td>
<td>Specifies the type of IP address of the secondary remote system log server.</td>
</tr>
<tr>
<td>SecondarySyslogAddress</td>
<td>Specifies the IP address of the secondary remote system log server to send system log messages to.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enables or disables the remote logging of system messages.</td>
</tr>
</tbody>
</table>
Variable | Value
--- | ---
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

**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.
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.

**EDM MIB Web page navigation**

- [Using the EDM MIB Web page for SNMP Get and Get-Next](#) on page 126
- [Using the EDM MIB Web page for SNMP walk](#) on page 127

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

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

**Procedure steps**

1. From the navigation tree, double-click **Administration**.
2. In the Administration tree, double-click **MIB Web Page**.
3. In the **MIB Name/ OID** box, enter the object name or OID.
4. Click **Get**.
The result of the request appears in the Result area of the window. If the request is unsuccessful, a description of the received error appears.

5. Click **Get Next** to retrieve the information of the next object in the MIB.
6. Repeat step 3 as required.

---

**Using the EDM MIB Web page for SNMP walk**

You can use SNMP walk to retrieve a subtree of the MIB that has the SNMP object as root. Perform this procedure to request the result of MIB Walk.

**Procedure steps**

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

   The result of the request appears in the Result area. If the request is unsuccessful, a description of the received error appears.
Chapter 11: 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).

Navigation

- Configuring IPFIX globally using EDM on page 129
- Configuring IPFIX flows using EDM on page 130
- IPFIX collector management using EDM on page 132
- IPFIX port management using EDM on page 134
- Graphing IPFIX exporter statistics for a collector using EDM on page 138
- Viewing the IPFIX collector clear time using EDM on page 139

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

Use the data in this table to configure export flow information sources.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot (Unit)</td>
<td>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.</td>
</tr>
<tr>
<td>AgingIntv</td>
<td>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 have been updated. The records are deleted if no new updates are found between two checks.</td>
</tr>
<tr>
<td>ActiveTimeout</td>
<td>Indicates the flow record active timeout value in minutes. This is a read-only cell.</td>
</tr>
<tr>
<td>ExportIntv</td>
<td>Specifies the frequency of data exports to the collector in seconds. Values range from 10 to 3600 seconds.</td>
</tr>
<tr>
<td>ExportState</td>
<td>Enables or disables the exporter.</td>
</tr>
<tr>
<td>TempRefIntvSec</td>
<td>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.</td>
</tr>
<tr>
<td>TempRefIntvPkts</td>
<td>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.</td>
</tr>
</tbody>
</table>
IPFIX collector management using EDM

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

IPFIX collector management using EDM navigation

• Viewing IPFIX collectors using EDM on page 132
• Configuring IPFIX collectors using EDM on page 133
• Deleting IPFIX collectors using EDM on page 134

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

Use the data in this table to help you understand the IPFIX collectors display.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot (Unit)</td>
<td>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.</td>
</tr>
<tr>
<td>AddressType</td>
<td>Indicates the IP address type of the collector. Currently only IPv4 addresses are supported.</td>
</tr>
</tbody>
</table>
### Variable definitions

Use the data in this table to collect and analyze data exported from an IPFIX-compliant switch.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Indicates the IP address of the collector.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Indicates the protocol used to transport the IPFIX data to the collector. Currently only the UDP protocol is supported for this task.</td>
</tr>
<tr>
<td>DestPort</td>
<td>Indicates the port on which the collector is listening for IPFIX data. Currently only port 9995 is supported.</td>
</tr>
<tr>
<td>ProtoVer</td>
<td>Indicates the format in which IPFIX data is provided to the collector. Currently only Netflow version 9 formatting is supported.</td>
</tr>
<tr>
<td>Enable</td>
<td>Indicates the operational state of this collector.</td>
</tr>
</tbody>
</table>

#### 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

Use the data in this table to collect and analyze data exported from an IPFIX-compliant switch.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot (Unit)</td>
<td>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.</td>
</tr>
<tr>
<td>AddressType</td>
<td>Specifies the IP address type of the collector. Currently only IPv4 addresses are supported.</td>
</tr>
<tr>
<td>Address</td>
<td>Specifies the IP address of the collector.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Specifies the protocol used to transport the IPFIX data to the collector. Currently only the UDP protocol is supported for this task.</td>
</tr>
<tr>
<td>DestPort</td>
<td>Specifies the port on which the collector is listening for IPFIX data. Currently only port 9995 is supported.</td>
</tr>
<tr>
<td>ProtoVer</td>
<td>Specifies the format in which IPFIX data is provided to the collector. Currently only Netflow version 9 formatting is supported.</td>
</tr>
<tr>
<td>Enable</td>
<td>Enables or disables the collector.</td>
</tr>
</tbody>
</table>

**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.
IPFIX port management using EDM navigation

- Viewing IPFIX port information using EDM on page 135
- Modifying specific IPFIX port configurations using EDM on page 136
- Modifying all IPFIX port configurations using EDM on page 137

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

Use the data in this table to help you understand the IPFIX port display.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Indicates the individual port on which the IPFIX parameters are being configured. Ports are itemized in the Unit/Port format.</td>
</tr>
</tbody>
</table>
| 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. |
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

Use the data in this table to modify configuration parameters for specific IPFIX ports.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Specifies the individual port on which the IPFIX parameters are being configured. Ports are itemized in the Unit/Port format.</td>
</tr>
<tr>
<td>Flush</td>
<td>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:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• enable—IPFIX data is collected</td>
</tr>
<tr>
<td></td>
<td>• disable—IPFIX data is not collected</td>
</tr>
</tbody>
</table>
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

Use the data in this table to modify the IPFIX configuration parameters for all available ports.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• none—the port data is not flushed.</td>
</tr>
<tr>
<td></td>
<td>• flush—the port data is flushed, which deletes the data from switch memory.</td>
</tr>
<tr>
<td></td>
<td>• exportAndFlush—the port data is exported to a configured collector and the data is then flushed.</td>
</tr>
<tr>
<td>AllTraffic</td>
<td>Specifies if IPFIX data is collected on this port.</td>
</tr>
<tr>
<td></td>
<td>• enable—IPFIX data is collected</td>
</tr>
<tr>
<td></td>
<td>• disable—IPFIX data is not collected</td>
</tr>
</tbody>
</table>
### Variable and Value Table

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
</table>
| 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 |

### 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

Use the data in this table to graph IPFIX exporter statistics for a collector.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OutPkts</td>
<td>Indicates the total number of packets sent.</td>
</tr>
<tr>
<td>OutOctets</td>
<td>Indicates the total number of bytes sent.</td>
</tr>
<tr>
<td>PktsLoss</td>
<td>Indicates the total number of records lost.</td>
</tr>
</tbody>
</table>

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.