AVAYA

Monitoring Performance

Release 4.3
NN47500-701
Issue 01.01
March 2016

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

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

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage

Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such

Contents

Chapter 1: New in this document

Monitoring Performance is a new document for Release 4.3 so all the features are new in this release. See *Release Notes* for a full list of features.

Chapter 2: Performance management fundamentals

Performance management includes the management tools and features that are available to monitor and manage your routing switch.

Switch management tools

Use Command Line Interface or Enterprise Device Manager to access, manage, and monitor the switch.

Command Line Interface

To access the Command Line Interface (CLI) initially, you need a direct connection to the system from a terminal or PC. After you enable Telnet, you can access the CLI from a Telnet session on the network.

CLI contains commands to configure system operations and management access. CLI has five major command modes with different privileges.

For more information about CLI, see *Using CLI and EDM*.

Enterprise Device Manager

Enterprise Device Manager (EDM) is a Web-based graphical user interface (GUI) tool that operates with a Web browser. Use it to access, manage, and monitor a single system on your network from various locations within the network.

For more information about EDM, see *Using CLI and EDM*.

Dynamic network applications

Remote access services supported on the switch, such as, the File Transfer Protocol (FTP), Trivial FTP (TFTP), rlogin, and Telnet, use daemons. These remote access daemons are not enabled by default to enhance security.

After you disable a daemon flag, all existing connections abruptly terminate, and the daemon remains idle (accepts no connection requests).

Use the following dynamic network applications to manage remote access services:

- Access policies
- Port lock
- CLI access
- SNMP community strings
- Web management interface access

For more information about how to enable remote access services, see *Quick Start Configuration*.

For more information about how to access policies, lock a port, access the CLI, and configure SNMP community strings, see *Configuring Security*.

For more information about how to access the Web management interface, see *Using CLI and EDM*.

Digital diagnostic monitoring

Use Digital Diagnostic Monitoring (DDM) to monitor laser operating characteristics such as temperature, voltage, current, and power. This feature works at any time during active laser operation without affecting data traffic.

Three supported optical transceiver form factors support DDM:

- Small Form Factor Pluggable (SFP)
- 10 Gigabit Small Form Factor Pluggable plus (SFP+)
- Quad Small Form Factor Pluggable plus (QSFP+)

Note:

Different hardware platforms can support different form factors. For more information, see the hardware documentation for your platform.

Digital Diagnostic Interface (DDI) is an interface that supports DDM. These devices provide real-time monitoring of individual DDI SFPs, SFP+s, and QSFP+s on a variety of products. The DDM software provides warnings or alarms after the temperature, voltage, laser bias current, transmitter power or receiver power fall outside of vendor-specified thresholds during initialization.

Chapter 3: Chassis performance management using EDM

Use Enterprise Device Manager (EDM) to configure chassis parameters and to graph chassis statistics on the switch.

Viewing system performance

About this task

For information about how to use Key Health Indicators functionality to view system performance, see *Managing Faults*.

Viewing the trap sender table

About this task

Use the Trap Sender Table tab to view source and receiving addresses.

Procedure

1. On the Device physical view, select a chassis.
2. In the navigation tree, expand the following folders: **Configuration** > **Edit**.
3. Click **Chassis**.
4. Click the **Trap Sender Table** tab.

Trap Sender Table field descriptions

Use the data in the following table to use the **Trap Sender Table** tab.

Name	Description
RecvAddress	IP address for the trap receiver. This is a read-only parameter that contains the IP address configured in the TAddress field in the TargetTable.
SrcAddress	Source IP address to use when sending traps. This IP address will be inserted into the source IP address field in the UDP trap packet.

Chapter 4: Port performance management using CLI

This section contains procedures to configure port performance management in the CLI.

Viewing DDI port information

Perform this procedure to view basic SFP, SFP+, and QSFP+ manufacturing information and characteristics, and the current configuration.

About this task

This command displays information for DDI SFPs, SFP+s and QSFP+s.

Note:

Slot and port information can differ depending on hardware platform. Different hardware platforms can support different form factors. For more information, see the hardware documentation for your platform.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View basic SFP, SFP+, and QSFP+ manufacturing information and characteristics:

   ```
   show pluggable-optical-modules basic [{slot/port[/sub-port][-slot/port[/sub-port]][,...]}]
   ```

3. View configuration information:

   ```
   show pluggable-optical-modules config
   ```

4. View detailed SFP, SFP+, and QSFP+ manufacturing information and characteristics:

   ```
   show pluggable-optical-modules detail [{slot/port[/sub-port][-slot/port[/sub-port]][,...]}]
   ```

Example

```
Switch:1#show pluggable-optical-modules config

================================================================================
```

```
                  Pluggable Optical Module Global Configuration
================================================================================
                            ddm-monitor : disabled
                     ddm-monitor-interval : 5
                           ddm-traps-send : enabled
                       ddm-alarm-portdown : disabled
```

Variable definitions

Use the data in the following table to use the `show pluggable-optical-modules basic` and `show pluggable-optical-modules detail` commands.

Table 1: Variable definitions

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Viewing DDI temperature information

Perform this procedure to view SFP, SFP+, and QSFP+ temperatures.

Note:

Slot and port information can differ depending on hardware platform. Different hardware platforms can support different form factors. For more information, see the hardware documentation for your platform.

About this task

This command displays information for DDI SFPs, SFP+s, and QSFP+s.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View SFP, SFP+, and QSFP+ temperatures:

   ```
   show pluggable-optical-modules temperature [{slot/port[/sub-port][-
   slot/port[/sub-port]][,...]}]
   ```

Example

```
Switch:1#show pluggable-optical-modules temperature

================================================================================
                    Pluggable Optical Module Temperature(C)
================================================================================
PORT         LOW_ALARM LOW_WARN    ACTUAL   HIGH_WARN HIGH_ALARM THRESHOLD
NUM          THRESHOLD THRESHOLD   VALUE    THRESHOLD THRESHOLD  STATUS
--------------------------------------------------------------------------------
1/2             7.0       1.1250   65.2539    0.0       3.0156  Low Alarm
1/3             7.0       1.1250   65.2539    0.0       3.0156  Low Alarm
1/9             7.0625    0.0      65.2539    0.0       3.0156  Low Alarm
1/15            7.0625    0.0      65.2539    0.0       3.0156  Low Alarm
2/1             7.0625    0.0      65.2539    0.0       3.0156  Low Alarm
2/17            7.0625    0.0      65.2539    0.0       3.0156  Low Alarm
2/40            7.0625    0.0      65.2539    0.0       3.0156  Low Alarm
```

Variable definitions

Use the data in the following table to use the `show pluggable-optical-modules temperature` command.

Table 2: Variable definitions

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Viewing DDI voltage information

Perform this procedure to view SFP, SFP+, and QSFP+ voltages.

Note:

Slot and port information can differ depending on hardware platform. Different hardware platforms can support different form factors. For more information, see the hardware documentation for your platform.

About this task

This command displays information for DDI SFPs, SFP+s, and QSFP+s.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. View SFP, SFP+, and QSFP+ voltages:

```
show pluggable-optical-modules voltage [{slot/port[/sub-port][-slot/
port[/sub-port]][,...]}]
```

Example

```
Switch:1#show pluggable-optical-modules voltage

================================================================================
                      Pluggable Optical Module Voltage(V)
================================================================================
PORT         LOW_ALARM LOW_WARN    ACTUAL  HIGH_WARN HIGH_ALARM THRESHOLD
NUM          THRESHOLD THRESHOLD   VALUE   THRESHOLD THRESHOLD  STATUS
--------------------------------------------------------------------------------
1/2             0.1281    0.0       1.2596    0.5376    1.6396  Normal
1/3             0.0001    0.0       1.2596    0.3072    1.6396  Normal
1/9             0.0006    0.0       1.2596    2.6368    0.0     Normal
1/15            0.0006    0.0       1.2596    2.6368    0.0     Normal
2/1             0.0006    0.0       1.2596    2.6368    0.0     Normal
2/17            0.0006    0.0       1.2596    2.6368    0.0     Normal
2/40            0.0006    0.0       1.2596    2.6368    0.0     Normal
```

Variable definitions

Use the data in the following table to use the `show pluggable-optical-modules voltage` command.

Table 3: Variable definitions

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Chapter 5: Port performance management using EDM

This section describes port performance management functions on the switch.

Configuring rate limits

About this task

Configure the rate limit of broadcast or multicast packets to determine the total bandwidth limit on the port.

Procedure

1. On the Device Physical View, select a port or multiple ports.
2. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. Click the **Rate Limiting** tab.
5. Configure the parameters as required.
6. Click **Apply**.

Rate Limiting field descriptions

Use the data in the following table to use the **Rate Limiting** tab.

Name	Description
Index	The port number.
TrafficType	The type of traffic being rate limited, either broadcast or multicast traffic. The default is broadcast.
AllowedRatePps	This variable is the allowed traffic rate limit for the port in packets per second.

Table continues…

Name	Description
	For the switch, 1 to 25 sets the limit in a percentage of the total bandwidth on the port from 1–25 percent. On gigabit ports and MDAs, there can be up to a 2 percent difference between the configured and actual rate limiting values. For the switch, 1–65535 sets the limit in packets for each second.
Enable	Double-click in the field and select to enable (True) or disable (False) rate limiting. The default is false.

Viewing DDI information

About this task

You can view DDI information (such as port information, temperature and voltages) for SFPs and SFP+s in the 1/10 Gbps interface ports and for QSFP+s in 40 Gbps interface ports.

Note:

Slot and port information can differ depending on hardware platform. Different hardware platforms can support different form factors. For more information, see the hardware documentation for your platform.

Procedure

1. In the Physical Device view, select a port.
2. In the navigation pane, expand the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. Select the **DDI/SFP** tab.

DDI/SFP field descriptions

Use the data in the following table to use the **DDI/SFP** tab.

Name	Description
ConnectorType	Indicates the type of SFP, SFP+, or QSFP+ connector.
SupportsDDM	Indicates if the SFP, SFP+, or QSFP+ supports DDM.
DdmStatusMask	Indicates if DDM is enabled.
CLEI	Indicates the Telcordia register assignment CLEI code.

Table continues…

Name	Description
VendorName	Indicates the name of the SFP, SFP+, or QSFP+ manufacturer.
VendorPartNumber	Indicates the part number for the SFP, SFP+, or QSFP+.
VendorRevNumber	Indicates the manufacturer revision level for the SFP, SFP +, or QSFP+.
VendorSN	Indicates the manufacturer serial number for the SFP, SFP +, or QSFP+.
VendorDateCode	Indicates the manufacturer date code for the SFP, SFP+, or QSFP+.
Wavelength	Indicates the wavelength in nm of the SFP, SFP+, or QSFP+. This is valid for optical transceivers only.
Calibration	Indicates if the calibration is internal or external.
PowerMeasure	Indicates Rx power measurement as average or OMA.
Aux1Monitoring	Indicates if auxiliary monitoring is implemented for the SFP +.
Aux2Monitoring	Indicates if auxiliary monitoring is implemented for the SFP +.
TemperatureLowAlarmThreshold	Indicates the low alarm threshold in degrees Celsius.
TemperatureLowWarningThreshold	Indicates the high warning threshold in degrees Celsius.
Temperature	Indicates the current temperature in degrees Celsius of the SFP, SFP+, or QSFP+.
TemperatureHighWarningThreshold	Indicates the high warning threshold in degrees Celsius.
TemperatureHighAlarmThreshold	Indicates the high alarm threshold in degrees Celsius.
TemperatureStatus	Indicates if any temperature thresholds were exceeded.
VoltageLowAlarmThreshold	Indicates the low alarm threshold in volts.
VoltageLowWarningThreshold	Indicates the high warning threshold in volts.
Voltage	Indicates the current voltage in volts.
VoltageHighWarningThreshold	Indicates the high warning threshold in volts.
VoltageHighAlarmThreshold	Indicates the high alarm threshold in volts.
VoltageStatus	Indicates if any voltage thresholds were exceeded.
BiasLowAlarmThreshold	Indicates the bias current low alarm threshold in mA.
BiasLowWarningThreshold	Indicates the bias current high warning threshold in mA.
Bias	Indicates the laser bias current in mA.
BiasHighWarningThreshold	Indicates the bias current high warning threshold in mA.
BiasHighAlarmThreshold	Indicates the bias current high alarm threshold in mA.
BiasStatus	Indicates if any bias thresholds were exceeded.
TxPowerLowAlarmThreshold	Indicates the low alarm threshold in mW for the Tx power.

Table continues…

Name	Description
TxPowerLowWarningThreshold	Indicates the high warning threshold in mW for the Tx power.
TxPower	Indicates the current Tx power in mW.
TxPowerHighWarningThreshold	Indicates the high warning threshold in mW for the Tx power.
TxPowerHighAlarmThreshold	Indicates the high alarm threshold in mW for the Tx power.
TxPowerStatus	Indicates if any Tx power thresholds were exceeded.
RxPowerLowAlarmThreshold	Indicates the low alarm threshold in mW for the Rx power.
RxPowerLowWarningThreshold	Indicates the high warning threshold in mW for the Rx power.
RxPower	Indicates the current Rx power in mW.
RxPowerHighWarningThreshold	Indicates the high warning threshold in mW for the Rx power.
RxPowerHighAlarmThreshold	Indicates the high alarm threshold in mW for the Rx power.
RxPowerStatus	Indicates if any Rx power thresholds were exceeded.
Aux1LowAlarmThreshold	Indicates the low alarm threshold auxiliary 1 reading.
Aux1LowWarningThreshold	Indicates the high warning threshold auxiliary 1 reading.
Aux1	Indicates the current auxiliary 1 reading.
Aux1HighWarningThreshold	Indicates the high warning threshold auxiliary 1 reading.
Aux1HighAlarmThreshold	Indicates the high alarm threshold auxiliary 1 reading.
Aux1Status	Indicates if any auxiliary 1 thresholds were exceeded.
Aux2LowAlarmThreshold	Indicates the low alarm threshold auxiliary 2 reading.
Aux2LowWarningThreshold	Indicates the high warning threshold auxiliary 2 reading.
Aux2	Indicates the current auxiliary 2 reading.
Aux2HighWarningThreshold	Indicates the high warning threshold auxiliary 2 reading.
Aux2rHighAlarmThreshold	Indicates the high alarm threshold auxiliary 2 reading.
Aux2Status	Indicates if any auxiliary 2 thresholds were exceeded.

Note:

1. Threshold and actual values for TxBias, TxPower, and RxPower are provided for all 4 channels in QSFP+ optical transceivers.
2. Auxiliary monitoring does not apply to QSFP+s.

Chapter 6: Remote Monitoring

This section provides information on Remote Monitoring (RMON).

RMON has two versions:

- RMON1

  Note:

  The switch does not support RMON1.

- RMON2

RMON 2

Remote Monitoring (RMON) is a management information base (MIB) or a group of management objects that you use to obtain or configure values using the Simple Network Management Protocol (SNMP).

Use CLI or EDM, to globally enable RMON on the system.

After you globally enable RMON, you enable monitoring for individual devices on a port-by-port basis.

The RMON2 feature monitors network and application layer protocols on configured network hosts, either VLAN or port interfaces, that you enable for monitoring. The RMON2 feature expands the capacity of RMON1 to upper layer protocols in the OSI model.

The following figure shows which form of RMON monitors which layers in the OSI model:

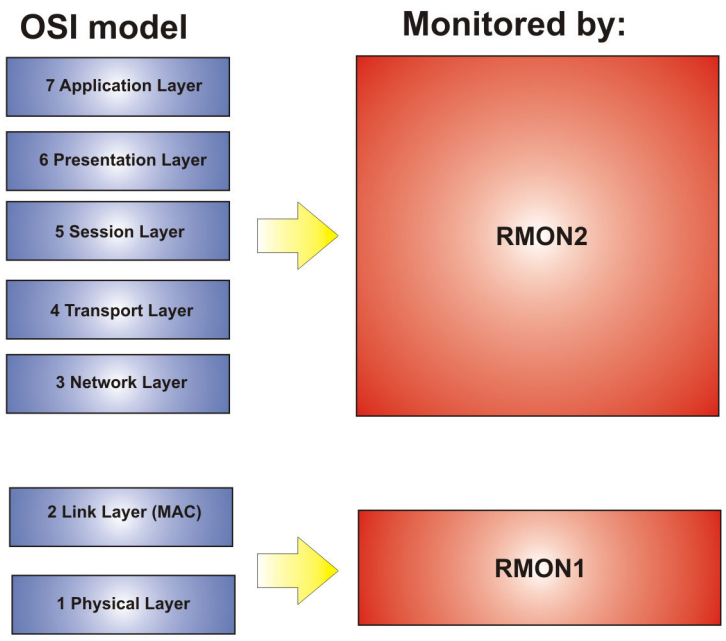

Figure 1: OSI model and RMON

The RMON2 feature is a management information base (MIB) or a group of management objects that you use to obtain or configure values using the Simple Network Management Protocol (SNMP). The switch supports a partial implementation of RMON2. The RMON2 feature adds the following MIBS: protocol directory, protocol distribution, address map, network-layer host and application layer host for the traffic passing through the (Control Processor) CP for these MIB tables.

The system only collects statistics for IP packets that pass through the CP. RMON2 does not monitor packets on other interfaces processed on the switch that do not pass through the CP.

After you globally enable RMON2, enable monitoring for individual devices. Identify the network hosts for the system to monitor with a manual configuration on the interfaces you want to monitor.

The RMON2 feature monitors a list of predefined protocols. The system begins to collect protocol statistics immediately after you enable RMON.

The RMON2 feature collects statistics on:

- Protocols predefined by the system.
- Address mapping between physical and network address on particular network hosts that you configure for monitoring.
- Network host statistics for particular hosts on a network layer protocol (IP) that you configure for monitoring.
- Application host statistics for a particular host on an application layer protocol that you configure for monitoring.

RMON2 MIBs

This section describes the following MIBs, on which RMON2 can collect statistics: protocol directory, protocol distribution, address map, network-layer host, and application layer host.

Protocol directory MIB

The protocol directory is a master directory that lists all of the protocols RMON2 can monitor. The protocols include network layer, transport layer, and application layer protocols, under the OSI model. The system only monitors statistics for the predefined protocols. You cannot delete or add additional protocols to this table. The protocol directory MIB is enabled by default for the predefined protocols.

The predefined protocols include:

- Internet Protocol (IP)
- Secure Shell version 2 (SSHv2)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Telnet
- Remote login (rlogin)
- Trivial File Transfer Protocol (TFTP)
- Simple Network Management Protocol (SNMP)

Protocol distribution MIB

The protocol distribution MIB collects traffic statistics that each protocol generates by local area network (LAN) segment. The switch acts as the probe and the system collects protocol statistics for the entire switch as part of the group for all of the protocols predefined in the protocol directory table. The protocol distribution control table is part of this group. The protocol distribution control table is predefined with an entry for the management IP for the switch to represent the network segment where the system collects the statistics.

No CLI or EDM support exists to add or delete entries in this table.

Address map MIB

The address map MIB maps the network layer IP to the MAC layer address.

The system populates the address map control table MIB with an entry for each host interface that you enable for monitoring on the switch.

Network layer host MIB

The network layer host MIB monitors the Layer 3 traffic statistics for each host. The network layer host MIB monitors traffic packets in and out of hosts based on the network layer address. The network layer host controls the network and application layer host tables.

The system populates an entry for the management IP of the switch to represent the network segment where the system collects the statistics. You have to enable each host interface that you want to monitor on the switch.

The system only collects statistics for this group from packets that go to the CP.

Application layer host MIB

The application layer host MIB monitors traffic statistics by application protocol for each host.

The system populates an entry for the management IP of the switch to represent the network segment where the system collects the statistics. You have to enable each host interface that you want to monitor on the switch.

The system only collects statistics for this group from packets that go to the CP.

RMON configuration using CLI

This section contains procedures to configure RMON using Command Line Interface (CLI).

Enabling RMON globally

Enable RMON globally, and then enable RMON on the host interfaces you want to monitor. By default, RMON is disabled globally.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Enable RMON globally:

   ```
   rmon
   ```

Example

Configure RMON globally:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#rmon
```

Enabling Remote Monitoring on an interface

Use the following procedure to enable Remote Monitoring (RMON) on an interface.

Before you begin

- Enable RMON globally.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable RMON on a particular VLAN:

```
vlan rmon <1-4059>
```

3. Enter GigabitEthernet Interface Configuration mode:

```
enable
configure terminal
interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
```

Note:

If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

4. Enable RMON on a particular port:

```
rmon
```

Example

Enable RMON on VLAN 2:

```
Switch:1>enable
Switch:1#configure terminal
Switch1:1(config)#vlan rmon 2
```

Enable RMON on port 3/8:

Note:

Slot and port information can differ depending on hardware platform. For more information, see the hardware documentation for your platform.

```
Switch:1>enable
Switch:1#configure terminal
Switch1:1(config)#interface gigabitethernet 3/8
Switch1:1(config-if)#rmon
```

Variable definitions

Use the data in this table to use the **`vlan rmon`** command.

Variable	Value
<1-4059>	Specifies the VLAN ID on which to configure RMON.

Displaying RMON information

View RMON information on the switch such as the RMON address maps, application host statistics, control tables, network host statistics, and protocol distribution statistics.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RMON2 information:

```
show rmon {address-map|application-host-stats WORD<1-64>|ctl-table|
network-host-stats|protocol-dist-stats}
```

Variable definitions

Use the data in the following table to use the **`show rmon`** command.

Variable	Value
address-map	Displays the RMON2 address map. This RMON2 parameter expands RMON capacity to display information on network, transport, and application layers.
application-host-stats *WORD<1–64>*	Displays RMON2 application host statistics from one of the following protocols: TCP, UDP, FTP, Telnet HTTP, rLogin, SSHv2, TFTP, SNMP, HTTPS. This RMON2 parameter expands RMON capacity to display network, transport, and application layers.
ctl-table	Displays the RMON2 control tables. This RMON2 parameter expands RMON capacity to display network, transport, and application layers.
network-host-stats	Displays RMON2 network-host statistics. This RMON2 parameter expands RMON capacity to display network, transport, and application layers.
protocol-dist-stats	Displays RMON2 protocol distribution statistics. This RMON2 parameter expands RMON capacity to display network, transport, and application layers.

Displaying RMON status

View the current RMON status on the switch.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RMON status:

```
show rmon
```

Example

```
Switch: show rmon

RMON Info :
Status       : enable
```

Displaying RMON address maps

View the maps of network layer address to physical address to interface.

The probe adds entries based on the source MAC and network addresses in packets without MAC-level errors.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RMON address maps:

   ```
   show rmon address-map
   ```

Example

```
Switch: show rmon address-map
================================================================================
                              Rmon Address Map Table
================================================================================
PROTOIDX  HOSTADDR         SOURCE  PHYADDR            LASTCHANGE
--------------------------------------------------------------------------------
1         12.1.1.1         2060    b0:ad:aa:42:a5:03  10/09/15 17:30:41
```

Job aid

The following table describes the fields in the output for the **`show rmon address-map`** command.

Parameter	Description
PROTOIDX	Shows a unique identifier for the entry in the table.
HOSTADDR	Shows the network address for this entry. The format of the value depends on the protocol portion of the local index.
SOURCE	Shows the interface or port on which the network address was most recently seen.
PHYADDR	Shows the physical address on which the network address was most recently seen.
LASTCHANGE	Shows when the entry was created or last changed. If this value changes frequently, it can indicate duplicate address problems.

Displaying RMON application host statistics

View application host statistics to see traffic statistics by application protocol for each host.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RMON application host statistics:

   ```
   show rmon application-host-stats WORD<1-64>
   ```

Example

```
Switch:# show rmon application-host-stats ?
  WORD<1-64>  Select one of these application protocols
              {TCP|UDP|FTP|TELNET|HTTP|RLOGIN|SSH|TFTP|SNMP|HTTPS}
Switch:# show rmon application-host-stats FTP

================================================================================
                          Rmon Application Host Stats
================================================================================
HOSTADDR         INPKT      OUTPKT     INOCT      OUTOCT     CREATETIME
--------------------------------------------------------------------------------
12.1.1.1         0          0          0          0          10/09/15 17:29:54
```

Job aid

The following table describes the fields in the output for the **`show rmon application-host-stats`** command.

Parameter	Description
HOSTADDR	Shows the network address for this entry. The format of the value depends on the protocol portion of the local index.
INPKT	Shows the number of packets for this protocol type, without errors, transmitted to this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times.
OUTPKT	Shows the number of packets for this protocol type, without errors, transmitted by this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times.
INOCT	Shows the number of octets transmitted to this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames.
OUTOCT	Shows the number of octets transmitted by this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames.
CREATETIME	Shows when the entry was last activated.

Displaying RMON control tables

View RMON control tables to see the data source for both network layer and application layer host statistics.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RMON control tables:

   ```
   show rmon ctl-table
   ```

Job aid

The following table describes the fields in the output for the **show rmon ctl-tabl** command.

Parameter	Description
ADDRMAPCFG	Describes and configures the probe support for the network layer and application layer host tables for this protocol. The value can be one of the following: • **NOT SUPPORTED** • **SUPPORTED OFF** • **SUPPORTED ON** If the value is **SUPPORTED ON**, the probe adds entries to the address map table that maps the network layer address to the MAC layer address.
AHDROPFRAMES	Shows the total number of application layer host frames that the probe receives and drops. This value does not include packets that were not counted because they had MAC-layer errors.
CREATETIME	Shows when the entry was last activated.
DATASOURCE	Shows the source of data for the entry.
DROPFRAMES	Shows the total number of frames that the probe receives and drops. This value does not include packets that were not counted because they had MAC-layer errors.
HOSTCFG	Describes and configures the probe support for the network layer and application layer host tables for this protocol. The value can be one of the following: • **NOT SUPPORTED** • **SUPPORTED OFF** • **SUPPORTED ON** If the value is **SUPPORTED ON**, the probe adds entries to the Host Control table to collect statistics for network layer and application layer hosts.
IDX	Shows a unique identifier for the entry in the table.
MATRIXCFG	Describes and configures the probe support for the network layer and application layer host tables for this protocol. The value can be one of the following: • **NOT SUPPORTED** • **SUPPORTED OFF** • **SUPPORTED ON**
NHDROPFRAMES	Shows the total number of network host frames that the probe receives and drops. This value does not include packets that were not counted because they had MAC-layer errors.
OWNER	Shows the entity that configured this entry.

Table continues…

Parameter	Description
PROTOCOL	Shows the protocols RMON2 can monitor: • Internet Protocol (IP) • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP) • File Transfer Protocol (FTP) • Secure Shell version 2 (SSHv2) • Telnet • Hypertext Transfer Protocol (HTTP) • Remote login (RLOGIN) • Trivial File Transfer Protocol (TFTP) • Simple Networking Management Protocol (SNMP) • Hypertext Transfer Protocol Secure (HTTPS)

Displaying RMON network host statistics

View network host statistics to see Layer 3 traffic statistics for each host. The network layer host MIB monitors traffic packets in and out of hosts based on the network layer address.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RMON network host statistics:

```
show rmon network-host-stats
```

Job aid

The following table describes the fields in the output for the **`show rmon network-host-stats`** command.

Parameter	Description
HOSTADDR	Shows the host address for this entry.
INPKT	Shows the number of packets without errors transmitted to this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times.
OUTPKT	Shows the number of packets without errors transmitted by this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times.

Table continues…

Parameter	Description
INOCT	Shows the number of octets transmitted to this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames.
OUTOCT	Shows the number of octets transmitted by this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames.
CREATETIME	Shows when the entry was last activated.

Displaying RMON protocol distribution statistics

View protocol distribution statistics to see traffic statistics that each protocol generates by local area network (LAN) segment.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RMON protocol distribution statistics:

   ```
   show rmon protocol-dist-stats
   ```

Example

```
Switch: show rmon protocol-dist-stats

================================================================================
                            Rmon Protocol Dist Stats
================================================================================
PROTOCOL  PKTS       OCTETS
--------------------------------------------------------------------------------
IP        0          0
TCP       0          0
UDP       0          0
FTP       0          0
SSH       0          0
TELNET    0          0
HTTP      0          0
RLOGIN    0          0
TFTP      0          0
SNMP      0          0
HTTPS     0          0
```

RMON configuration using EDM

Remote monitoring (RMON) is a management information base (MIB) or a group of management objects that you use to obtain or configure values using the Simple Network Management Protocol (SNMP).

Enabling RMON globally

About this task

Enable RMON globally, and then enable RMON on the host interfaces you want to monitor. By default, RMON is disabled globally.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Options**.
3. Click the **Options** tab.
4. Select the **Enable** check box.
5. Click **Apply**.

Options field descriptions

Use the data in the following table to use the **Options** tab.

Name	Description
Enable	Enables RMON. If you select the **Enable** check box, the RMON agent starts immediately. To disable RMON, clear the **Enable** check box and click **Apply** to save the new setting to NVRAM, and then restart the device. The default is disabled.

Enabling RMON on a port or VLAN

Use the following procedure to enable RMON on an interface.

Before you begin

- Enable RMON globally.

Procedure

1. Enable RMON on a VLAN:
   a. In the navigation pane, expand the following folders: **Configuration** > **VLAN**.
   b. Click **VLANs**.
   c. Click the **Advanced** tab.
   d. In the row for the VLAN, double-click the **RmonEnable** field, and then select **enable**.
   e. Click **Apply**.
2. Enable RMON on a port:
   a. In the Device Physical View, select a port.

b. In the navigation pane, expand the following folders: **Configuration** > **Edit** > **Port**.
c. Click **General**.
d. Click the **Interface** tab.
e. For the **RmonEnable** field, select **enable**.
f. Click **Apply**.

Viewing the protocol directory

View the protocol directory to see the list of protocols that RMON2 can monitor. You cannot change the list of protocols.

About this task

The protocol directory MIB is enabled by default for the predefined protocols.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Protocol Directory**.
3. Click the **Protocol Directories** tab.

Protocol Directories field descriptions

Use the data in the following table to use the **Protocol Directories** tab.

Name	Description
Index	Shows a unique identifier for the entry in the table.
Protocol	Shows the protocols RMON2 can monitor: • Internet Protocol (IP) • Secure Shell version 2 (SSHv2) • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP) • File Transfer Protocol (FTP) • Hypertext Transfer Protocol (HTTP) • Telnet • Remote login (rlogin) • Trivial File Transfer Protocol (TFTP) • Simple Networking Management Protocol (SNMP)

Table continues…

Name	Description
AddressMapConfig	Describes and configures the probe support for the network layer and application layer host tables for this protocol. The value can be one of the following: • notSupported • supportedOff • supportedOn If the value is supportedOn, the probe adds entries to the Address Map tab that maps the network layer address to the MAC layer address.
HostConfig	Describes and configures the probe support for the network layer and application layer host tables for this protocol. The value can be one of the following: • notSupported • supportedOff • supportedOn If the value is supportedOn, the probe adds entries to the Host Control tab to collect statistics for network layer and application layer hosts.
MatrixConfig	Describes and configures the probe support for the network layer and application layer host tables for this protocol. The value can be one of the following: • notSupported • supportedOff • supportedOn
Owner	Shows the entity that configured this entry.

Viewing the data source for protocol distribution statistics

View the Distribution Control tab to see the network segment data source on which the protocol distribution statistics are measured. The management IP mentioned as a data source represents the IP that the SNMP agent uses to access the switch.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Protocol Distribution**.
3. Click the **Distribution Control** tab.

Distribution Control field descriptions

Use the data in the following table to use the **Distribution Control** tab.

Name	Description
Index	Shows a unique identifier for the entry in the table.
DataSource	Specifies the source of data for this protocol distribution.
DroppedFrames	Shows the total number of frames that the probe receives and drops but does not include in the StatsDropEvents value. This event can occur if the probe is out of resources and sheds the load from this collection. This value does not include packets that were not counted because they had MAC-layer errors.
CreateTime	Shows the value of the sysUpTime when the entry was last activated.
Owner	Shows the entity that configured this entry.

Viewing protocol distribution statistics

View protocol distribution statistics to see traffic statistics that each protocol generates by local area network (LAN) segment.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Protocol Distribution**.
3. Click the **Distribution Stats** tab.

Distribution Stats field descriptions

Use the data in the following table to use the **Distribution Stats** tab.

Name	Description
LocalIndex	Identifies the protocol distribution an entry is part of, as well as the particular protocol that it represents.
Pkts	Shows the number of packets without errors received for this protocol type. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times.

Table continues…

Name	Description
Octets	Shows the number of octets in packets received for this protocol type since it was added to the table. This value does not include octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames.

Viewing the host interfaces enabled for monitoring

View the entries in the address map control tab to see which host interfaces are enabled for monitoring on the switch. Each entry in this table enables the discovery of addresses on a new interface.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Address Map**.
3. Click the **Address Map Control** tab.

Address Map Control field descriptions

Use the data in the following table to use the **Address Map Control** tab.

Name	Description
Index	Shows a unique identifier for the entry in the table.
DataSource	Shows the source of data for the entry.
DroppedFrames	Shows the total number of frames that the probe receives and drops but does not include in the StatsDropEvents value. This event can occur if the probe is out of resources and sheds the load from this collection. This value does not include packets that were not counted because they had MAC-layer errors.
Owner	Shows the entity that configured this entry.

Viewing address mappings

View the mappings of network layer address to physical address to interface.

About this task

The probe adds entries on this tab based on the source MAC and network addresses in packets without MAC-level errors.

The probe populates this table for all protocols on the **Protocol Directories** tab with a value of **AddressMapConfig** equal to **supportedOn**.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Address Map**.
3. Click the **Address Map** tab.

Address Map field descriptions

Use the data in the following table to use the **Address Map** tab.

Name	Description
LocalIndex	Shows a unique identifier for the entry in the table.
HostAddress	Shows the network address for this entry. The format of the value depends on the protocol portion of the local index.
Source	Shows the interface or port on which the network address was most recently seen.
PhysicalAddress	Shows the physical address on which the network address was most recently seen.
LastChange	Shows the value of the sysUpTime when the entry was created or last changed. If this value changes frequently, it can indicate duplicate address problems.

Viewing the data source for host statistics

View the Host Control tab to see the data source for both network layer and application layer host statistics.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Network Layer Host**.
3. Click the **Host Control** tab.

Host Control field descriptions

Use the data in the following table to use the **Host Control** tab.

Name	Description
Index	Shows a unique identifier for the entry in the table.
DataSource	Shows the source of data for the associated host table. The statistics in this group reflect all packets on the local network segment that attaches to the identified interface.
NHDropFrames	Shows the total number of frames that the probe receives and drops but does not include in the StatsDropEvents value. This event can occur if the probe is out of resources and sheds the load from this collection. This value does not include packets that were not counted because they had MAC-layer errors.
AHDropFrames	Shows the total number of frames that the probe receives and drops but does not include in the StatsDropEvents value. This event can occur if the probe is out of resources and sheds the load from this collection. This value does not include packets that were not counted because they had MAC-layer errors.
Owner	Shows the entity that configured this entry.

Viewing network host statistics

View network host statistics to see Layer 3 traffic statistics for each host. The network layer host MIB monitors traffic packets in and out of hosts based on the network layer address.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Network Layer Host**.
3. Click the **Network Host Stats** tab.

Network Host Stats field descriptions

Use the data in the following table to use the **Network Host Stats** tab.

Name	Description
LocalIndex	Shows a unique identifier for the entry in the table.
HostAddress	Shows the host address for this entry.
InPkts	Shows the number of packets without errors transmitted to this address. This value is the number of link-layer packets so a single, fragmented

Table continues…

Name	Description
	network-layer packet can increment the counter several times.
OutPkts	Shows the number of packets without errors transmitted by this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times.
InOctets	Shows the number of octets transmitted to this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames.
OutOctets	Shows the number of octets transmitted by this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames.
CreateTime	Shows the value of the sysUpTime when the entry was last activated.

Viewing application host statistics

View application host statistics to see traffic statistics by application protocol for each host.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Serviceability** > **RMON**.
2. Click **Application Layer Host**.
3. Click the **Application Host Stats** tab.

Application Host Stats field descriptions

Use the data in the following table to use the **Application Host Stats** tab.

Name	Description
Index	Shows a unique identifier for the entry in the table.
HostAddress	Identifies the network layer address of this entry.
LocalIndex	Identifies the network layer protocol of the address.
InPkts	Shows the number of packets for this protocol type, without errors, transmitted to this address. This value is the number of link-layer packets so a single,

Table continues…

Name	Description
	fragmented network-layer packet can increment the counter several times.
OutPkts	Shows the number of packets for this protocol type, without errors, transmitted by this address. This value is the number of link-layer packets so a single, fragmented network-layer packet can increment the counter several times.
InOctets	Shows the number of octets transmitted to this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames.
OutOctets	Shows the number of octets transmitted by this address, excluding octets in packets that contained errors. This value counts octets in the entire packet that contained the protocol, not just the particular protocol frames.
CreateTime	Shows the value of the sysUpTime when the entry was last activated.

Chapter 7: MACsec performance

MACsec statistics

This feature is not supported on all hardware platforms. For more information about feature support, see *Release Notes*.

MAC Security (MACsec) is an IEEE 802® standard that allows authorized systems in a network to transmit data confidentially and to take measures against data transmitted or modified by unauthorized devices.

The switch supports the following statistics that provide a measure of MACsec performance.

Table 4: General MACsec statistics

Statistics	Description
TxUntaggedPkts	Specifies the number of transmitted packets without the MAC security tag (SecTAG), with MACsec disabled on the interface.
TxTooLongPkts	Specifies the number of transmitted packets discarded because the packet length is greater than the Maximum Transmission Unit (MTU) of the Common Port interface.
RxUntaggedPkts	Specifies the number of received packets without the MAC security tag (SecTAG), with MACsec *not* operating in strict mode.
RxNoTagPkts	Specifies the number of received packets without the MAC security tag (SecTAG), with MACsec operating in strict mode.
RxBadTagPkts	Specifies the number of received packets discarded with an invalid SecTAG or with a zero value Packet Number (PN)/invalid Integrity Check Value (ICV).
RxUnknownSCIPkts	Specifies the number of packets received with an unknown Secure Channel Identifier (SCI) and with MACsec *not* operating in strict mode.
RxNoSCIPkts	Specifies the number of packets received with an unknown Secure Channel Identifier (SCI) and with MACsec operating in strict mode.
RxOverrunPkts	Specifies the number of packets discarded because the number of received packets exceeded the cryptographic performance capabilities.

Table 5: Secure-channel inbound MACsec statistics

Statistics	Description
UnusedSAPkts	Specifies the summation of received unencrypted packets on all SAs of this secure channel, with MACsec *not* in strict mode.

Table continues…

Statistics	Description
NoUsingSAPkts	Specifies the summation of received packets that were discarded along with either encrypted packets or packets that were received with MACsec operating in strict mode.
LatePkts	Specifies the number of packets received that have been discarded for this Secure Channel (SC) with Replay Protect enabled. **Note:** The current release does not support Replay Protect.
NotValidPkts	Specifies the summation of packets that were discarded in all SAs of the SC because they were not valid with one of the following conditions: • MACsec was operating in strict mode • The packets received were encrypted but contained erroneous fields.
InvalidPkts	Specifies the summation of all packets received that were not valid for this SC, with MACsec operating in *check* mode.
DelayedPkts	Specifies the summation of packets for this SC, with the Packet Number (PN) of the packets lower than the lower bound replay protection PN. **Note:** The current release does not support Replay Protect.
UncheckedPkts	The total number of packets for this SC that: • were encrypted and had failed the integrity check • were *not* encrypted and had failed the integrity check • were received when MACsec validation was not enabled
OKPkts	Specifies the total number of valid packets for all SAs of this Secure Channel.
OctetsValidated	Specifies the number of octets of plaintext recovered from received packets that were integrity protected but not encrypted.
OctetsDecrypted	Specifies the number of octets of plaintext recovered from received packets that were integrity protected and encrypted.

Table 6: Secure-channel outbound MACsec statistics

Statistics	Description
ProtectedPkts	Specifies the number of integrity protected but not encrypted packets for this transmitting SC.
EncryptedPkts	Specifies the number of integrity protected and encrypted packets for this transmitting SC.
OctetsProtected	Specifies the number of plain text octets that are integrity protected but not encrypted on the transmitting SC.
OctetsEncrypted	Specifies the number of plain text octets that are integrity protected and encrypted on the transmitting SC.

Viewing MACsec statistics using the CLI

Use the following procedure to view MAC Security (MACsec) statistics using CLI.

Viewing MACsec statistics

Perform this procedure to view the MACsec statistics.

This feature is not supported on all hardware platforms. If you do not see this command in EDM, the feature is not supported on your hardware. For more information about feature support, see *Release Notes*.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the general MACsec statistics:

   ```
   show macsec statistics [{slot/port[/sub-port][-slot/port[/sub-port]]
   [,...]}]
   ```

3. View the secure-channel inbound MACsec statistics:

   ```
   show macsec statistics [{slot/port[/sub-port][-slot/port[/sub-port]]
   [,...]}] secure-channel inbound
   ```

4. View the secure-channel outbound MACsec statistics:

   ```
   show macsec statistics [{slot/port[/sub-port][-slot/port[/sub-port]]
   [,...]}] secure-channel outbound
   ```

Example

Display general MACsec statistics, inbound MACsec statistics, and outbound MACsec statistics:

Note:

Slot and port information can differ depending on hardware platform. For more information, see the hardware documentation for your platform.

```
Switch:1>enable
Switch:1#show macsec statistics 1/40

================================================================================
                              MACSEC Port Statistics
================================================================================
        TxUntagged       TxTooLong       RxUntagged      RxNoTag
PortId   Packets          Packets         Packets        Packets
--------------------------------------------------------------------------------
1/40       0               0               0               0

          RxBadTag      RxUnknown       RxNoSCI       RxOverrun
PortId    Packets       SCIPackets      Packets        Packets
--------------------------------------------------------------------------------
```

```
1/40       0               0               0               0
```

```
Switch:1#show macsec statistics 1/40 secure-channel inbound

================================================================================
                  MACSEC Port Inbound Secure Channel Statistics
================================================================================
           UnusedSA     NoUsingSA       Late         NotValid      Invalid
PortId     Packets      Packets        Packets       Packets       Packets
--------------------------------------------------------------------------------
1/40       0               0               0           100037        0

           Delayed     Unchecked        Ok         Octets          Octets
PortId     Packets      Packets        Pkts      Validated       Decrypted
--------------------------------------------------------------------------------
1/40       0               0               0         53528828      0
```

```
Switch:1#show macsec statistics 1/40 secure-channel outbound

================================================================================
                  MACSEC Port Outbound Secure Channel Statistics
================================================================================
          Protected      Encrypted      Octets          Octets
PortId     Packets        Packets      Protected       Encrypted
--------------------------------------------------------------------------------
1/40       0               99946           0               53434154
```

Viewing MACsec statistics using EDM

Use the following procedures to view MAC Security (MACsec) statistics using EDM.

Viewing MACsec interface statistics

Use this procedure to view the MACsec interface statistics using EDM.

This feature is not supported on all hardware platforms. If you do not see this command in EDM, the feature is not supported on your hardware. For more information about feature support, see *Release Notes*.

Procedure

1. In the Device Physical View tab, select the port for which you need to view the MACsec interface statistics.
2. In the navigation tree, expand the following folders: **Edit** > **Port** > **General**.
3. Click the **MacSec Interface Stats** tab.

Note:

Use the **Clear Stats** button to the clear MACsec interface statistics. The **Clear Stats** button is available to clear single-port as well as multiple-port MACsec interface statistics.

MacSec interface field descriptions

The following table describes the fields in the **MacSec Interface Stats** tab.

Field	Description
TxUntaggedPkts	Specifies the number of transmitted packets without the MAC security tag (SecTAG), with MACsec disabled on the interface.
TxTooLongPkts	Specifies the number of transmitted packets discarded because the packet length is greater than the maximum transmission unit (MTU) of the common port interface.
RxUntaggedPkts	Specifies the number of received packets without the MAC security tag (SecTAG), with MACsec *not* operating in strict mode.
RxNoTagPkts	Specifies the number of received packets without the MAC security tag (SecTAG), with MACsec operating in strict mode.
RxBadTagPkts	Specifies the number of received packets discarded with an invalid SecTAG, or with a zero value packet number (PN), or invalid Integrity Check Value (ICV).
RxUnknownSCIPkts	Specifies the number of packets received with an unknown secure channel identifier (SCI), and with MACsec *not* operating in strict mode.
RxNoSCIPkts	Specifies the number of packets received with an unknown secure channel identifier (SCI), and with MACsec operating in strict mode.
RxOverrunPkts	Specifies the number of packets discarded because the number of received packets exceeded the cryptographic performance capabilities.

Viewing secure channel (SC) inbound statistics

Use this procedure to view the secure channel (SC) inbound statistics using EDM.

This feature is not supported on all hardware platforms. If you do not see this command in EDM, the feature is not supported on your hardware. For more information about feature support, see *Release Notes*.

Procedure

1. In the Device Physical View tab, select the port for which you need to view the SC inbound statistics.
2. In the navigation pane, expand the following folders: **Edit** > **Port** > **General**.
3. Click the **SC Inbound Stats** tab.

Note:

Use the **Clear Stats** button to the clear single-port secure channel inbound statistics. The **Clear Stats** button is not available to clear multiple-port secure channel inbound statistics.

SC Inbound Stats field descriptions

The following table describes the fields in the **SC Inbound Stats** tab.

Field	Description
UnusedSAPkts	Specifies the summary of received unencrypted packets on all SAs of this secure channel, with MACsec *not* in strict mode.
NoUsingSAPkts	Specifies the summary of received packets that were discarded along with either encrypted packets or packets that were received with MACsec operating in strict mode.
LatePkts	Specifies the number of packets received that have been discarded for this secure channel (SC) with Replay Protect enabled. **Note:** The current release does not support Replay Protect.
NotValidPkts	Specifies the summary of packets that were discarded in all SAs of the SC because they were not valid with one of the following conditions: • MACsec was operating in strict mode. • The packets received were encrypted but contained erroneous fields.
InvalidPkts	Specifies the summary of all packets received that were not valid for this SC, with MACsec operating in *check* mode.
DelayedPkts	Specifies the summary of packets for this SC, with the packet number (PN) of the packets lower than the lower bound replay protection PN. **Note:** The current release does not support Replay Protect.
UncheckedPkts	The total number of packets for this SC that: • Were encrypted and had failed the integrity check. • Were *not* encrypted and had failed the integrity check.

Table continues…

Field	Description
	• Were received when MACsec validation was not enabled.
OKPkts	Specifies the total number of valid packets for all SAs of this secure channel.
OctetsValidated	Specifies the number of octets of plaintext recovered from received packets that were integrity protected but not encrypted.
OctetsDecrypted	Specifies the number of octets of plaintext recovered from received packets that were integrity protected and encrypted.

Viewing secure channel (SC) outbound statistics

Use this procedure to view the secure channel (SC) outbound statistics using EDM.

This feature is not supported on all hardware platforms. If you do not see this command in EDM, the feature is not supported on your hardware. For more information about feature support, see *Release Notes*.

Procedure

1. In the Device Physical View tab, select the port for which you need to view the SC outbound statistics.
2. In the navigation tree, expand the following folders: **Edit** > **Port** > **General**.
3. Click the **SC Outbound Stats** tab.

Note:

Use the **Clear Stats** button to the clear single-port secure channel outbound statistics. The **Clear Stats** button is not available to clear multiple-port secure channel outbound statistics.

SC Outbound Stats field descriptions

The following table describes the fields in the **SC Outbound Stats** tab.

Field	Description
ProtectedPkts	Specifies the number of integrity protected but not encrypted packets for this transmitting SC.
EncryptedPkts	Specifies the number of integrity protected and encrypted packets for this transmitting SC.
OctetsProtected	Specifies the number of plain text octets that are integrity protected but not encrypted on the transmitting SC.

Table continues…

Field	Description
OctetsEncrypted	Specifies the number of plain text octets that are integrity protected and encrypted on the transmitting SC.

Chapter 8: Statistics

This chapter provides the procedures for using statistics to help monitor the performance of the switch using Enterprise Device Manager (EDM) and command line interface (CLI).

Viewing statistics using CLI

This section contains procedures to view statistics in the CLI.

Viewing TCP statistics

View TCP statistics to manage network performance.

Procedure

View TCP statistics:

```
show ip tcp statistics
```

Example

```
Switch:#show ip tcp statistics
show ip tcp global statistics:
------------------
ActiveOpens:        0
PassiveOpens:       37
AttemptFails:       0
EstabResets:        34
CurrEstab:          1
InSegs:             6726
OutSegs:            7267
RetransSegs:        10
InErrs:             0
OutRsts:            10
```

Job aid

The following table describes the output for the **`show ip tcp statistics`** command.

Table 7: show ip tcp statistics command output

Field	Description
ActiveOpens	The count of transitions by TCP connections to the SYN-SENT state from the CLOSED state.
PassiveOpens	The count of transitions by TCP connections to the SYN-RCVD state from the LISTEN state.
AttemptFails	The count of transitions by TCP connections to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the count of transitions to the LISTEN state from the SYN-RCVD state.
EstabResets	The count of transitions by TCP connections to the CLOSED state from the ESTABLISHED or CLOSE-WAIT state.
CurrEstab	The count of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
InSegs	The total count of segments received, including those received in error. This count includes segments received on currently established connections.
OutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
RetransSegs	The total count of TCP segments transmitted containing one or more previously transmitted octets.
InErrs	The count of segments received in error.
OutRsts	The count of TCP segments sent containing the RST flag.

Displaying DHCP-relay statistics for specific ports

Display individual DHCP-relay statistics for specific ports to manage network performance.

Note:

Slot and port information can differ depending on hardware platform.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View DHCP-relay statistics for a specific port or VRF.

   ```
   show interfaces GigabitEthernet statistics dhcp-relay [vrf
   WORD<1-16>] [vrfids WORD<0-512>]|{slot/port[/sub-port][-slot/port[/
   sub-port]][,...]}}
   ```

Example

View DHCP-relay statistics:

```
Switch:1>enable
Switch:1#show interfaces gigabitethernet statistics dhcp-relay

================================================================================
                                Port Stats Dhcp
================================================================================
PORT_NUM VRF NAME         NUMREQUEST NUMREPLY
--------------------------------------------------------------------------------
1/12     GlobalRouter     0          2
1/13     GlobalRouter     3          2
2/3      GlobalRouter     0          2
--------------------------------------------------------------------------------
```

Variable definitions

Use the data in the following table to use the **`show interfaces GigabitEthernet statistics dhcp-relay`** command.

Variable	Value
vrf *WORD<1-16>*	Specifies a VRF instance by VRF name.
vrfids *WORD<0-512>*	Specifies the ID of the VRF.
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (1/1). Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Job aid

The following table describes parameters for the **`show interfaces GigabitEthernet statistics dhcp-relay`** command output.

Table 8: show interfaces gigabitethernet statistics dhcp-relay field descriptions

Variable	Value
PORT_NUM	Indicates the port number.
VRF NAME	Identifies the VRF
NUMREQUEST	Indicates the total number of DHCP requests on this interface
NUMREPLY	Indicates the total number of DHCP replies on this interface.

Displaying DHCP-relay statistics for all interfaces

About this task

Display DHCP-relay statistics for all interfaces to manage network performance.

Note:

Slot and port information can differ depending on hardware platform.

Procedure

1. Show the number of requests and replies for each interface:

   `show ip dhcp-relay counters [vrf WORD<1-16>] [vrfids WORD<0-512>]`

2. Show counters for Option 82:

   `show ip dhcp-relay counters option82 [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Example

```
Switch:>show ip dhcp-relay counters option82
================================================================================
                    DHCP Counters Option82 - GlobalRouter
================================================================================
          IP              FOUND DROP CIRC ADD  DEL  REMOTE             ADD   DEL
INTERFACE ADDR            OP82  PKT  ID   CIRC CIRC ID               REMID REMID
--------------------------------------------------------------------------------
Port 1/12  192.0.2.1      0     0    395  0     0   00:24:7f:9d:0a:00  0     0
Vlan40     192.0.10.1     0     0    2088 0     0   00:24:7f:9d:0a:01  0     0
```

Variable definitions

Use the data in the following table to use the **`show ip dhcp-relay counters`** command.

Variable	Value
vrf *WORD<1-16>*	Specifies a VRF instance by the VRF name.
vrfids *WORD<0-512>*	Specifies the ID of the VRF.

Job aid

The following table explains the output from the **`show ip dhcp-relay counters option82`** command.

Table 9: show ip dhcp-relay counters option82 command

Heading	Description
INTERFACE	Shows the name of the interface on which you enabled option 82. Shows the port number if the interface is a brouter port or the VLAN number if the interface is a VLAN.

Table continues…

Heading	Description
IP ADDR	Shows the IP address associated with the interface.
FOUND OPT82	Shows the number of packets that the interface received that already had option82 in them.
DROP PKT	Shows the number of packets the interface dropped because of option 82–related issues. These reasons could be that the packet was received from an untrusted source or spoofing was detected. To determine the cause of the drop, you must enable trace on level 170.
CIRCUIT ID	Show the value inserted in the packets as the circuit ID. The value is the index of the interface.
ADD CIRC	Shows on how many packets (requests from client to server) the circuit ID was inserted for that interface. If you expect this value to increase but it does not, and the interface does not drop a packet, it is possible the packet does not have enough space to insert the option. You must enable trace on level 170 to determine the cause.
REMOVE CIRC	Shows on how many packets (replies from server to client) the circuit id was removed for that interface.
REMOTE ID	Shows the value inserted in the packets as the remote ID. The value is the MAC address of the interface.
ADD REMOTE	Shows on how many packets (requests from client to server) the remote ID was inserted for that interface. If you expect this value to increase but it does not, and the interface does not drop a packet, it is possible the packet does not have enough space to insert the option. You must enable trace on level 170 to determine the cause.
REMOVE REMOTE	Shows on how many packets (replies from server to client) the remote ID was removed for that interface.

Displaying LACP statistics for specific ports

Display individual LACP statistics for specific ports to manage network performance.

Note:

Slot and port information can differ depending on hardware platform.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. View statistics for specific ports:

   ```
   show interfaces GigabitEthernet statistics lacp [{slot/port[/sub-port][-slot/port[/sub-port]][,...]}]
   ```

Example

View LACP statistics:

```
Switch:1>enable
Switch:1#show interfaces gigabitethernet statistics lacp

================================================================================
                                Port Stats Lacp
================================================================================
PORT TX     RX     TX         RX         TX             RX             RX      RX
NUM  LACPDU LACPDU MARKERPDU MARKERPDU MARKERRESPPDU MARKERRESPPDU UNKNOWN ILLEGAL
--------------------------------------------------------------------------------
1/39  0        0        0          0          0               0    0       0
1/40  0        0        0          0          0               0    0       0
2/37  0        0        0          0          0               0    0       0
2/38  0        0        0          0          0               0    0       0
```

Variable definitions

Use the data in the following table to use the **`show interfaces GigabitEthernet statistics lacp`** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Job aid

The following table describes parameters for the `show interfaces GigabitEthernet statistics lacp` command.

Table 10: show interfaces GigabitEthernet statistics lacp field descriptions

Parameter	Description
PORT_NUM	Indicates the port number.
TX LACPDU	The count of transmitted LACP data units.
RX LACPDU	The count of received LACP data units.
TX MARKERPDU	The count of transmitted marker protocol data units.
RX MARKERPDU	The count of received marker protocol data units.

Table continues…

Parameter	Description
TX MARKERRESPPDU	The count of transmitted marker protocol response data units.
RX MARKERRESPPDU	The count of received marker protocol response data units.
RX UNKNOWN	The count of received unknown frames.
RX ILLEGAL	The count of received illegal frames.

Displaying VLACP statistics for specific ports

Display VLACP statistics for specific ports to manage network performance.

Note:

Slot and port information can differ depending on hardware platform.

About this task

You can enable sequence numbers for each VLACPDU to assist in monitoring performance. The switch counts mismatched PDU sequence numbers to determine packet loss information. By default, sequence numbers are enabled.

You can use the show commands from Privileged EXEC mode but must enter Global Configuration mode to enable or disable the sequence numbers.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Confirm sequence numbers are enabled:

   ```
   show vlacp
   ```

3. **(Optional)** Enable sequence numbers for VLACPDUs:

   ```
   vlacp sequence-num
   ```

4. View VLACP statistics:

   ```
   show interfaces gigabitEthernet statistics vlacp [{slot/port[/sub-port][-slot/port[/sub-port]][,...]} ]
   ```

5. **(Optional)** View VLACP statistics history:

   ```
   show interfaces gigabitEthernet statistics vlacp history [{slot/port[/sub-port][-slot/port[/sub-port]][,...]} ]
   ```

6. **(Optional)** Clear VLACP statistics:

```
clear vlacp stats [port {slot/port[/sub-port][-slot/port[/sub-port]]
[,...]}]
```

7. **(Optional)** Disable sequence numbers for VLACPDUs:

```
no vlacp sequence-num
```

Example

Determine if sequence numbers are enabled, and then view port statistics. Port numbering may differ depending on your product and configuration.

```
Switch:1(config)#show vlacp

================================================================================
                            Vlacp Global Information
================================================================================
                SystemId: 32:11:9f:20:00:00
                   Vlacp: enable
   Vlacp Sequence Number: enable

Switch:1(config)#show interfaces gigabitEthernet statistics vlacp
================================================================================
                                Port Stats Vlacp
================================================================================
PORT        TX          RX          SEQNUM
NUM         VLACPDU     VLACPDU     MISMATCH
--------------------------------------------------------------------------------
8/1         106058      105554      0
12/11       15          12          0
12/23       0           0           0
```

Variable definitions

Use the data in the following table to use the commands in this procedure.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Job aid

The following table describes fields in the output for the **`show interfaces gigabitEthernet statistics vlacp`** command.

Field	Description
PORT NUM	Shows the slot and port number.
TX VLACPDU	Shows the number of VLACPDUs transmitted on the port.

Table continues…

Field	Description
RX VLACPDU	Shows the number of valid VLACPDUs received on the port.
SEQNUM MISMATCH	Shows the number of mismatched VLACPDUs in terms of received sequence numbers on the port.

Displaying RMON statistics for specific ports

Display individual RMON statistics for specific ports to manage network performance.

Note:

Slot and port information can differ depending on hardware platform.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View statistics for specific ports:

   ```
   show interfaces GigabitEthernet statistics rmon {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

Example

View RMON statistics:

```
Switch:1>enable
Switch:1#show interfaces gigabitEthernet statistics rmon 1/13

================================================================================
                                Port Stats Rmon
================================================================================
PORT  OCTETS     PKTS    MULTI   BROAD   CRC     UNDER   OVER    FRAG    COLLI
NUM                      CAST    CAST    ALLIGN  SIZE    SIZE    MENT    SION
--------------------------------------------------------------------------------
1/13  1943       21      8       13      0       0       0       0       0
```

Variable definitions

Use the data in the following table to use the **`show interfaces GigabitEthernet statistics rmon`** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Job aid

The following table describes parameters for the `show interfaces GigabitEthernet statistics rmon` command output.

Table 11: show interfaces GigabitEthernet statistics rmon field descriptions

Parameter	Description
PORT NUM	Indicates the port number.
OCTETS	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
PKTS	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
MULTICAST	The total number of packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
BROADCAST	The total number of packets received that were directed to the broadcast address. This number does not include multicast packets.
CRC ALLIGN	The total number of packets received that had a length (excluding framing bits, but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error), or a bad FCS with a nonintegral number of octets (Alignment Error).
UNDERSIZE	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
OVERSIZE	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
FRAGMENT	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
COLLISION	An estimated value for the total number of collisions on this Ethernet segment.

Displaying detailed statistics for ports

Display detailed statistics for specific ports to manage network performance.

Note:

Slot and port information can differ depending on hardware platform.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View statistics for specific ports:

   ```
   show interfaces GigabitEthernet statistics verbose {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

Example

View statistics for various ports:

```
Switch:1>enable
Switch:1#show interfaces gigabitethernet statistics verbose

Please widen the terminal for optimal viewing of data.

================================================================================================

                       Port Stats Interface Extended
================================================================================================

PORT_NUM IN_UNICST  OUT_UNICST IN_MULTICST OUT_MULTICST IN_BRDCST OUT_BRDCST IN_LSM OUT_LSM
------------------------------------------------------------------------------------------------

2/1      0          0          0           0            0          0          0      0
2/2      0          0          0           0            0          0          0      0
2/3      0          0          0           0            0          0          0      0
2/4      0          0          0           0            0          0          0      0
2/5      0          0          0           0            0          0          0      0
2/6      0          0          0           0            0          0          0      0
3/1      0          0          0           0            0          0          0      0
3/2      0          0          0           0            0          0          0      0
3/3      0          0          8702        34805        0          0          0      0
3/4      0          0          0           0            0          0          0      0
3/5      0          0          0           0            0          0          0      0
3/6      0          0          0           0            0          0          0      0
3/7      0          0          0           0            0          0          0      0
3/8      0          0          0           0            0          0          0      0
3/9      0          0          0           0            0          0          0      0

--More-- (q = quit)
```

Variable definitions

Use the data in the following table to use the **`show interfaces GigabitEthernet statistics verbose`** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of

Variable	Value
	slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Job aid

The following table describes parameters for the `show interfaces GigabitEthernet statistics verbose` command.

Table 12: how interfaces GigabitEthernet statistics verbose field descriptions

Parameter	Description
PORT_NUM	Indicates the port number.
IN_UNICAST	The count of inbound Unicast packets.
OUT_UNICAST	The count of outbound Unicast packets.
IN_MULTICAST	The count of inbound Multicast packets.
OUT_MULTICAST	The count of outbound Multicast packets.
IN_BRDCST	The count of inbound broadcast packets.
OUT_BRDCST	The count of outbound broadcast packets.

Displaying IS-IS statistics and counters

Use the following procedure to display the IS-IS statistics and counters.

Procedure

1. Display IS-IS system statistics:

   ```
   show isis statistics
   ```

2. Display IS-IS interface counters:

   ```
   show isis int-counters
   ```

3. Display IS-IS level 1 control packet counters:

   ```
   show isis int-l1-cntl-pkts
   ```

   Note:

   The current release uses level 1 IS-IS. The current release does not support level 2 IS-IS. The CLI command **`show isis int-l2-contl-pkts`** is not supported in the current release because the IEEE 802.1aq standard currently only defines the use of one hierarchy, Level 1.

4. Clear IS-IS statistics:

```
clear isis stats [error-counters] [packet-counters]
```

Example

```
Switch:# show isis statistics
================================================================================
                              ISIS System Stats
================================================================================

LEVEL    CORR   AUTH   AREA   MAX SEQ   SEQ NUM  OWN LSP  BAD ID  PART   LSP    DB
                LSPs  FAILS  DROP   EXCEEDED   SKIPS    PURGE    LEN    CHANGES OLOAD
--------------------------------------------------------------------------------
Level-1  0      0      0      0        1        0        0       0       0
```

```
Switch:# show isis int-counters
================================================================================
                           ISIS Interface Counters
================================================================================

IFIDX    LEVEL   AUTH     ADJ         INIT      REJ     ID LEN  MAX AREA LAN  DIS
                 FAILS    CHANGES       FAILS     ADJ                        CHANGES
--------------------------------------------------------------------------------
Mlt2     Level 1-2  0        1              0       0          0       0        0
Port1/21 Level 1-2  0        1              0       0          0       0        0
```

```
Switch:# show isis int-l1-cntl-pkts
================================================================================
                        ISIS L1 Control Packet counters
================================================================================
IFIDX         DIRECTION     HELLO        LSP          CSNP         PSNP

--------------------------------------------------------------------------------
Mlt2           Transmitted       13346        231          2            229
Mlt2           Received          13329        230          1            230
Port1/21       Transmitted       13340        227          2            226
Port1/21       Received          13335        226          1            227
```

Variable definitions

Use the data in the following table to use the **clear isis stats** command.

Variable	Value
error-counters	Clears IS-IS stats error-counters.
packet-counters	Clears IS-IS stats packet-counters.

Job aid

show isis statistics

The following table describes the fields in the output for the **show isis statistics** command.

Parameter	Description
LEVEL	Shows the level of the IS-IS interface (Level 1 in the current release).
CORR LSPs	Shows the number of corrupted LSPs detected.
AUTH FAILS	Shows the number of times authentication has failed on the global level.

Table continues…

Parameter	Description
AREA DROP	Shows the number of manual addresses dropped from the area.
MAX SEQ EXCEEDED	Shows the number of attempts to exceed the maximum sequence number.
SEQ NUM SKIPS	Shows the number of times the sequence number was skipped.
OWN LSP PURGE	Shows how many times the local LSP was purged.
BAD ID LEN	Shows the number of ID field length mismatches.
PART CHANGES	Shows the number of partition link changes.
LSP DB OLOAD	Show the number of times the switch was in the overload state.

show isis int-counters

The following table describes the fields in the output for the **`show isis int-counters`** command.

Parameter	Description
IFIDX	Shows the interface index for the Ethernet or MLT interface.
LEVEL	Shows the level of the IS-IS interface (Level 1 in the current release).
AUTH FAILS	Shows the number of times authentication has failed per interface.
ADJ CHANGES	Shows the number of times the adjacencies have changed.
INIT FAILS	Shows the number of times the adjacency has failed to establish.
REJ ADJ	Shows the number of times the adjacency was rejected by another router.
ID LEN	Shows the ID field length mismatches.
MAX AREA	Shows the maximum area address mismatches.
LAN DIS CHANGES	Shows the number of times the DIS has changed.

show isis int-l1-cntl-pkts

The following table describes the fields in the output for the **`show isis int-l1-cntl-pkts`** command.

Parameter	Description
IFIDX	Shows the interface index for the Ethernet or MLT interface.
DIRECTION	Shows the packet flow (Transmitted or Received).
HELLO	Shows the amount of interface-level Hello packets.
LSP	Shows the amount of LSP packets.
CSNP	Shows the amount of CSNPs.
PSNP	Shows the amount of PSNPs.

Clearing ACL statistics

Clear default ACL statistics if you no longer require previous statistics.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Enter the following command to clear default ACL statistics:

   ```
   clear filter acl statistics default [<1-2048>]
   ```

3. Enter the following command to clear global ACL statistics:

   ```
   clear filter acl statistics global [<1-2048>]
   ```

4. Enter the following command to clear all ACL statistics:

   ```
   clear filter acl statistics all
   ```

5. Enter the following command to clear statistics associated with a particular ACL, ACE, or ACE type:

   ```
   clear filter acl statistics [<1-2048>] [<1-2000>][qos] [security]
   ```

Variable definitions

Use the information in the following table to use the **`clear filter acl statistics`** command.

Variable	Value
1–2048	Specifies the ACL ID.
1–2000	Specifies the ACE ID.

Viewing ACE statistics

View ACE statistics to ensure that the filter operates correctly.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View ACE statistics for a specific ACL, ACE, or ACE type:

   ```
   show filter acl statistics <1-2048> [<1-2000>] [qos] [security]
   ```

3. View all ACE statistics:

   ```
   show filter acl statistics all
   ```

4. View default ACE statistics:

   ```
   show filter acl statistics default [<1-2048>]
   ```

5. View global statistics for ACEs:

   ```
   show filter acl statistics global [<1-2048>]
   ```

Example

View ACE statistics:

```
Switch:1>enable
Switch:1#show filter acl statistics all

================================================================================
                          Acl Global Statistics Table
================================================================================
Acl Id  Acl Name    Acl Type  Acl Sec    Acl Sec    Acl QOS    Acl QOS
                              Packets    Bytes      Packets    Bytes
--------------------------------------------------------------------------------
1       ACL-1       inVlan    0          0          0          0
2       ACL-2       inVlan    0          0          0          0

Displayed 2 of 2 entries


================================================================================
                          Acl Default Statistics Table
================================================================================
Acl Id  Acl Name    Acl Type  Acl Sec    Acl Sec    Acl QOS    Acl QOS
                              Packets    Bytes      Packets    Bytes
--------------------------------------------------------------------------------
1       ACL-1       inVlan    0          0          0          0
2       ACL-2       inVlan    0          0          0          0

Displayed 2 of 2 entries


--More-- (q = quit)

Switch:1#show filter acl statistics default

================================================================================
                          Acl Default Statistics Table
================================================================================
Acl Id  Acl Name    Acl Type  Acl Sec    Acl Sec    Acl QOS    Acl QOS
                              Packets    Bytes      Packets    Bytes
--------------------------------------------------------------------------------
1       ACL-1       inVlan    0          0          0          0
2       ACL-2       inVlan    0          0          0          0

Displayed 2 of 2 entries

Switch:1#show filter acl statistics global 2

================================================================================
                          Acl Global Statistics Table
================================================================================
Acl Id  Acl Name    Acl Type  Acl Sec    Acl Sec    Acl QOS    Acl QOS
                              Packets    Bytes      Packets    Bytes
--------------------------------------------------------------------------------
2       ACL-2       inVlan    0          0          0          0

Displayed 1 of 1 entries
```

Variable definitions

Use the data in the following table to use the **`show filter acl statistics`** command.

Variable	Value
1–2048	Specifies the ACL ID.
1–2000	Specifies the ACE ID.

Job aid

The following table describes output for the `show filter acl statistics default` command.

Table 13: show filter acl statistics default field descriptions

Parameter	Description
Acl ID	Specifies the identifier for the ACL.
Acl Name	Specifies the name for the ACL.
Acl Type	Specifies the ACL type.
Acl Sec Packets	Specifies the ACL secondary packets.
Acl Sec Bytes	Specifies the ACL secondary bytes.
Acl QoS Packets	Specifies the ACL QoS packets.
Acl QoS Bytes	Specifies the ACL QoS bytes.

Viewing MSTP statistics

About this task

Display MSTP statistics to see MSTP related bridge-level statistics.

Procedure

Display the MSTP related bridge-level statistics:

```
show spanning-tree mstp statistics
```

Example

```
Switch:#show spanning-tree mstp statistics

================================================================================
                            MSTP Bridge Statistics
================================================================================
Mstp UP Count                   : 1
Mstp Down Count                 : 0
Region Config Change Count      : 12
Time since topology change      : 8 day(s), 02H:54M:33S
Topology change count           : 10
New Root Bridge Count           : 25
```

Job aid

The following table describes the output for the `show spanning-tree mstp statistics` command.

Table 14: show spanning-tree mstp statistics field descriptions

Parameter	Description
MSTP Up Count	The number of times the MSTP port has been enabled. A Trap is generated on the occurrence of this event.
MSTP Down Count	The number of times the MSTP port has been disabled. A Trap is generated on the occurrence of this event.
Region Config Change Count	The number of times the switch detects a Region Configuration Identifier Change. The switch generates a trap on the occurrence of this event.
Time since topology change	The time (in hundredths of a second) since the TcWhile Timer for any port in this Bridge was non-zero for Common Spanning Tree context.
Topology change count	The count of at least one non zero TcWhile timers on this Bridge for Common Spanning Tree context.
New Root Bridge Count	The number of times this Bridge has detected a Root Bridge change for Common Spanning Tree context. A Trap is generated on the occurrence of this event.

Viewing RSTP statistics

About this task

View Rapid Spanning Tree Protocol statistics to manage network performance.

Procedure

View RSTP stats with the following command:

```
show spanning-tree rstp statistics
```

Job aid

The following table describes output for the **`show spanning-tree rstp statistics`** command.

Table 15: show spanning-tree rstp statistics field descriptions

Field	Description
RSTP Up Count	The number of times RSTP port has been enabled. A Trap is generated on the occurrence of this event.
RSTP Down Count	The number of times RSTP port has been disabled. A Trap is generated on the occurrence of this event.

Table continues…

Field	Description
Count of Root Bridge Changes	The number of times this Bridge has detected a Root Bridge change for Common Spanning Tree context.
STP Time since Topology change	The time (in hundredths of a second) since the "TcWhile" Timer for any port in this Bridge was non zero for this spanning tree instance.
Total number of topology changes	The number of times that there have been at least one non zero "TcWhile" Timer on this Bridge for this spanning tree instance.

Viewing RSTP port statistics

About this task

View RSTP statistics on ports to manage network performance.

Note:

Slot and port information can differ depending on hardware platform.

Procedure

View RSTP statistics on a port:

```
show spanning-tree rstp port statistics [{slot/port[/sub-port][-slot/
port[/sub-port]][,...]}]
```

Example

View RSTP statistics:

```
Switch:1#show spanning-tree rstp port statistics

================================================================================
                              RSTP Port Statistics
================================================================================
Port Number                          : 4/1
Number of Fwd Transitions            : 0
Rx RST BPDUs Count                   : 0
Rx Config BPDU Count                 : 0
Rx TCN BPDU Count                    : 0
Tx RST BPDUs Count                   : 0
Tx Config BPDU Count                 : 0
Tx TCN BPDU Count                    : 0
Invalid RST BPDUs Rx Count           : 0
Invalid Config BPDU Rx Count         : 0
Invalid TCN BPDU Rx Count            : 0
Protocol Migration Count             : 0
Port Number                          : 4/2
Number of Fwd Transitions            : 0
Rx RST BPDUs Count                   : 0
Rx Config BPDU Count                 : 0
Rx TCN BPDU Count                    : 0
Tx RST BPDUs Count                   : 0
Tx Config BPDU Count                 : 0

--More-- (q = quit)
```

Variable definitions

Use the data in the following table to use the **show spanning-tree rstp port statistics** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Job aid

The following table describes output for the `show spanning-tree rstp port statistics` command.

Table 16: show spanning-tree rstp port statistics field descriptions

Parameter	Description
RxRstBpduCount	The number of RSTP BPDUs received on this port.
RxConfigBpduCount	The number of configuration BPDUs received on this port.
RxTcnBpduCount	The number of TCN BPDUs received on this port.
TxRstBpduCount	The number of RSTP BPDUs transmitted by this port.
TxConfigBpduCount	The number of Config BPDUs transmitted by this port.
TxTcnBpduCount	The number of TCN BPDUs transmitted by this port.
InvalidRstBpduRxCount	The number of invalid RSTP BPDUs received on this port. A trap is generated on the occurrence of this event.
InvalidConfigBpduRx Count	The number of invalid configuration BPDUs received on this port. A trap is generated on the occurrence of this event.
InvalidTcnBpduRxCount	The number of invalid TCN BPDUs received on this port. A trap is generated on the occurrence of this event.
ProtocolMigrationCount	The number of times this port migrated from one STP protocol version to another. The relevant protocols are STP-Compatible and RSTP. A trap is generated on the occurrence of this event.

Viewing MLT statistics

About this task

View MLT statistics to display MultiLink Trunking statistics for the switch or for the specified MLT ID.

Procedure

View MLT statistics:

```
show mlt stats [<1-512>]
```

Example

```
Switch:#show mlt stats

================================================================================
                                Mlt Interface
================================================================================
ID IN-OCTETS          OUT-OCTETS         IN-UNICST          OUT-UNICST
--------------------------------------------------------------------------------
1  256676904          183670662          1397               456
2  61737348498        61584347982        1450182            1490619
4  229256124          47472778           0                  0
100 251678170          32332107           0                  0

ID IN-MULTICST        OUT-MULTICST       IN-BROADCST        OUT-BROADCST      MT
--------------------------------------------------------------------------------
1  2419514            2295274            41                 268194            E
2  962303832          960067410          765                237               E
4  2159884            666153             0                  90                E
100 2095269            504965             13                 0                 E
```

Variable definitions

Use the data in the following table to help you use the **`show mlt stats`** command.

Variable	Value
<1-512>	Specifies the MLT ID.

Job aid

The following table describes the output for the `show mlt stats` command.

Table 17: show mlt stats field descriptions

Parameter	Description
ID IN-OCTETS	The total number of inbound octets of data (including those in bad packets).
OUT-OCTETS	The total number of outbound octets of data.
IN-UNICAST	The count of inbound Unicast packets.
OUT-UNICAST	The count of outbound unicast packets.

Table continues…

Parameter	Description
ID IN-MULTICAST	The count of inbound multicast packets.
OUT-MULTICAST	The count of outbound multicast packets.
IN-BROADCAST	The count of inbound broadcast packets.
OUT-BROADCAST	The count of outbound broadcast packets.
MT	The MLT type: P for POS, E for Ethernet, A for ATM.

Viewing vIST statistics

View virtual IST (vIST) statistics for the switch.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display the vIST statistics:

   ```
   show virtual-ist stat
   ```

3. To clear the vIST statistics:

   ```
   clear virtual-ist stats
   ```

Example

```
Switch:1#show virtual-ist stat
================================================================================
                              IST Message Statistics
================================================================================
PROTOCOL MESSAGE            COUNT
--------------------------------------------------------------------------------

Ist Down                 :  0
Hello Sent               :  0
Hello Recv               :  0
Learn MAC Address Sent   :  0
Learn MAC Address Recv   :  0
MAC Address AgeOut Sent  :  0
MAC Address AgeOut Recv  :  0
MAC Address Expired Sent :  0
MAC Address Expired Sent :  0
Delete Mac Address Sent  :  0
Delete Mac Address Recv  :  0
Smlt Down Sent           :  0
Smlt Down Recv           :  0
Smlt Up Sent             :  0
Smlt Up Recv             :  0
Send MAC Address Sent    :  0
Send MAC Address Recv    :  0
IGMP Sent                :  0
IGMP Recv                :  0
Port Down Sent           :  0
Port Down Recv           :  0
Request MAC Table Sent   :  0
Request MAC Table Recv   :  0
```

```
Unknown Msg Type Recv    :  0
Mlt Table Sync Req Sent  :  0
Mlt Table Sync Req Recv  :  0
Mlt Table Sync Sent      :  0
Mlt Table Sync Recv      :  0
Port Update Sent         :  0
Port Update Recv         :  0
Entry Update Sent        :  0
Entry Update Recv        :  0
Dialect Negotiate Sent   :  0
Dialect Negotiate Recv   :  0
Update Response Sent     :  0
Update Response Recv     :  0
Transaction Que HiWaterM :  0
Poll Count Hi Water Mark :  0
```

Job aid

The following table describes the output for the `show virtual-ist stat` command.

Table 18: show virtual-ist stat field descriptions

Parameter	Description
Ist Down	The count of how many sessions between the two peering switches went down since last boot.
Hello Sent	The count of transmitted hello messages.
Hello Recv	The count of received hello messages.
Learn MAC Address Sent	The count of transmitted learned MAC address messages.
Learn MAC Address Recv	The count of received learned MAC address messages.
MAC Address AgeOut Sent	The count of transmitted aging out MAC address messages.
MAC Address AgeOut Recv	The count of received aging out MAC address messages.
MAC Address Expired Sent	The count of transmitted MAC address age expired messages.
MAC Address Expired Recv	The count of received MAC address age expired messages.
Delete Mac Address Sent	The count of transmitted MAC address deleted messages.
Delete Mac Address Recv	The count of received MAC address deleted messages.
Smlt Down Sent	The count of transmitted SMLT down messages.
Smlt Down Recv	The count of received SMLT down messages.
Smlt Up Sent	The count of transmitted SMLT up messages.
Smlt Up Recv	The count of received SMLT up messages.

Table continues…

Parameter	Description
Send MAC Address Sent	The count of transmitted send MAC table messages.
Send MAC Address Recv	The count of received send MAC table messages.
IGMP Sent	The count of transmitted IGMP messages.
IGMP Recv	The count of received IGMP messages.
Port Down Sent	The count of transmitted port down messages.
Port Down Recv	The count of received port down messages.
Request MAC Table Sent	The count of transmitted MAC table request messages.
Request MAC Table Recv	The count of received MAC table request messages.
Unknown Msg Type Recv	The count of received unknown message type messages.
Mlt Table Sync Req Sent	The count of transmitted MLT table sync request messages.
Mlt Table Sync Req Recv	The count of received MLT table sync request messages.
Mlt Table Sync Sent	The count of transmitted MLT table sync messages.
Mlt Table Sync Recv	The count of received MLT table sync messages.
Port Update Sent	The count of transmitted port update messages.
Port Update Recv	The count of received port update messages.
Entry Update Sent	The count of transmitted entry update messages.
Entry Update Recv	The count of received entry update messages.
Dialect Negotiate Sent	The count of transmitted protocol ID messages.
Dialect Negotiate Recv	The count of received protocol ID messages.
Update Response Sent	The count of transmitted update response messages.
Update Response Recv	The count of received update response messages.
Transaction Que HiWaterM	The count of transaction queue high watermark messages.
Poll Count Hi Water Mark	The count of poll count high watermark messages.

Showing RADIUS server statistics

Before you begin

- To clear statistics, you must log on to at least the Privileged EXEC mode.

About this task

You cannot collect the following network statistics from a console port: the number of input and output packets, and the number of input and output bytes. All other statistics from console ports are available to assist with debugging.

Procedure

1. Display RADIUS server statistics:

   ```
   show radius-server statistics
   ```

2. Clear server statistics:

   ```
   clear radius statistics
   ```

Example

```
Switch:#show radius-server statistics

Responses with invalid server address: 0

   Radius Server(UsedBy) : 47.17.143.58(cli)
-----------------------------------------------------------
         Access Requests : 52
          Access Accepts : 0
          Access Rejects : 0
           Bad Responses : 52
          Client Retries : 52
        Pending Requests : 0
        Acct On Requests : 1
       Acct Off Requests : 0
     Acct Start Requests : 47
      Acct Stop Requests : 46
   Acct Interim Requests : 0
      Acct Bad Responses : 94
   Acct Pending Requests : 0
     Acct Client Retries : 94
       Access Challanges : 0
         Round-trip Time :
          Nas Ip Address : 47.17.10.32

   Radius Server(UsedBy) : 47.17.143.58(snmp)
-----------------------------------------------------------
         Access Requests : 0
          Access Accepts : 0
          Access Rejects : 0
           Bad Responses : 0
          Client Retries : 0
        Pending Requests : 0
        Acct On Requests : 0
       Acct Off Requests : 0
     Acct Start Requests : 0
      Acct Stop Requests : 0
   Acct Interim Requests : 0
      Acct Bad Responses : 0
   Acct Pending Requests : 0
     Acct Client Retries : 0
       Access Challanges : 0
         Round-trip Time :
          Nas Ip Address : 47.17.10.32

--More-- (q = quit)
```

Job aid

The following table shows the field descriptions for the `show radius-server statistics` command output.

Table 19: show radius-server statistics command fields

Parameter	Description
RADIUS Server	The IP address of the RADIUS server.
AccessRequests	Number of access-response packets sent to the server; does not include retransmissions.
AccessAccepts	Number of access-accept packets, valid or invalid, received from the server.
AccessRejects	Number of access-reject packets, valid or invalid, received from the server.
BadResponses	Number of invalid access-response packets received from the server.
PendingRequests	Access-request packets sent to the server that have not yet received a response, or have timed out.
ClientRetries	Number of authentication retransmissions to the server.
AcctOnRequests	Number of accounting On requests sent to the server.
AcctOffRequests	Number of accounting Off requests sent to the server.
AcctStartRequests	Number of accounting Start requests sent to the server.
AcctStopRequests	Number of accounting Stop requests sent to the server.
AcctInterimRequests	Number of accounting Interim Requests sent to the server. The AcctInterimRequests counter increments only if the parameter acct-include-cli-commands is set to true.
AcctBadResponses	Number of Invalid Responses from the server that are discarded.
AcctPendingRequests	Number of requests waiting to be sent to the server.
AcctClientRetries	Number of retries made to this server.

Showing OSPF error statistics on a port

Use statistics to help you monitor Open Shortest Path First (OSPF) performance. You can also use statistics in troubleshooting procedures.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display extended information about OSPF errors for the specified port or for all ports:

   ```
   show interfaces GigabitEthernet error ospf [{slot/port[/sub-port][-slot/port[/sub-port]][,...]}]
   ```

Variable definitions

Use the following table to help you use the **`show interfaces GigabitEthernet error ospf`** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Job aid

The following table describes the output for the **`show interfaces GigabitEthernet error ospf`** command.

Table 20: show interfaces GigabitEthernet error ospf field descriptions

Parameters	Description
PORT NUM	Indicates the port number.
VERSION MISMATCH	Indicates the number of version mismatches this interface receives.
AREA MISMATCH	Indicates the number of area mismatches this interface receives.
AUTHTYPE MISMATCH	Indicates the number of AuthType mismatches this interface receives.
AUTH FAILURES	Indicates the number of authentication failures.
NET_MASK MISMATCH	Indicates the number of net mask mismatches this interface receives.
HELLOINT MISMATCH	Indicates the number of hello interval mismatches this interface receives.
DEADINT MISMATCH	Indicates the number of dead interval mismatches this interface receives.
OPTION MISMATCH	Indicates the number of options mismatches this interface receives.

Viewing OSPF interface statistics

Use statistics to help you monitor Open Shortest Path First (OSPF) performance. You can also use statistics in troubleshooting procedures.

This command is not available on all hardware platforms.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display OSPF interface statistics:

   ```
   show ip ospf ifstats [detail vrf WORD<1-16> vrfids WORD<0-512>]
   [mismatch vrf WORD<1-16> vrfids WORD<0-512>] [vlan <1-4059>] [vrf
   WORD<1-16>] [vrfids WORD<0-512>]
   ```

Example

```
Switch:#show ip ospf ifstats
```

```
================================================================================
                    OSPF Interface Statistics - GlobalRouter
================================================================================
               ---HELLOS---- ---DBS--- -LS REQ-- --LS UPD--- --LS ACK---
INTERFACE      RX     TX     RX   TX   RX   TX   RX    TX     RX    Tx
--------------------------------------------------------------------------------
2.2.2.32       76035  76355  33   32   4    9    2483  2551   2525  1247
30.30.30.32    76038  76349  0    0    0    0    0     0      0     0
40.1.1.32      153207 76355  38   44   6    11   2899  3797   4203  1601
```

Variable definitions

Use this table to help you use the **`show ip ospf ifstats`** command.

Variable	Value
detail	Shows detailed information.
mismatch	Shows the number of times the area ID is not matched.
vlan *<1-4059>*	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
vrf *WORD<1-16>*	Specifies a VRF instance by VRF name.
vrfids *WORD<0-512>*	Specifies a VRF or range of VRFs by ID.

Job aid

The following table describes the output for the **`show ip ospf ifstats`** command.

Table 21: show ip ospf ifstats field descriptions

Field	Description
INTERFACE	Indicates the IP address of the host.
HELLOS RX	Indicates the number of hello packets received by this interface.
HELLOS TX	Indicates the number of hello packets transmitted by this interface.
DBS RX	Indicates the number of database descriptor packets received by this interface.
DBS TX	Indicates the number of database descriptor packets transmitted by this interface.
LS REQ	Indicates the number of link state request packets received by this interface.
LS TX	Indicates the number of link state request packets transmitted by this interface.
LS UDP RX	Indicates the number of link state update packets received by this interface.
LS UDP TX	Indicates the number of link state update packets transmitted by this interface.

Table continues…

Field	Description
LS ACK RX	Indicates the number of link state acknowledge packets received by this interface.
LS ACK TX	Indicates the number of link state acknowledge packets transmitted by this interface.
VERSION	Indicates the OSPF version.
AREA	Indicates the OSPF area.
AUTHTYPE	Indicates the OSPF authentication type.
AUTHFAIL	The count of authentication fail messages.
NETMASK	Indicates the net mask.
HELLO	The count of Hello messages.
DEADTRR OPTION	The dead TRR option.

Viewing OSPF range statistics

Use statistics to help you monitor Open Shortest Path First (OSPF) performance. You can also use statistics in troubleshooting procedures. OSPF range statistics include area ID, range network address, range subnet mask, range flag, and LSDB type.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the OSPF range statistics:

   `show ip ospf stats [vrf WORD<1-16>] [vrfids WORD<0-512>]`

Example

```
Switch:#show ip ospf stats
================================================================================
                          OSPF Statistics - GlobalRouter
================================================================================
       NumBufAlloc: 239603
        NumBufFree: 239603
   NumBufAllocFail: 0
    NumBufFreeFail: 0
           NumTxPkt: 239655
           NumRxPkt: 317562
      NumTxDropPkt: 0
      NumRxDropPkt: 0
       NumRxBadPkt: 0
         NumSpfRun: 47
        LastSpfRun: 2 day(s), 04:18:58
       LsdbTblSize: 16
     NumAllocBdDDP: 24
      NumFreeBdDDP: 24
       NumBadLsReq: 0
    NumSeqMismatch: 3
     NumOspfRoutes: 4
      NumOspfAreas: 1
NumOspfAdjacencies: 3
```

```
--More-- (q = quit)
```

Variable definitions

Use the data in the following table to use the **show ip ospf stats** command.

Variable	Value
vrf *WORD<1-16>*	Specifies a VRF instance by VRF name.
vrfids *WORD<0-512>*	Specifies a VRF or range of VRFs by ID.

Job aid

The following table describes the show command output.

Table 22: show ip ospf stats command parameters

Parameter	Description
NumBufAlloc	Indicates the number of buffers allocated for OSPF.
NumBufFree	Indicates the number of buffers that are freed by the OSPF.
NumBufAllocFail	Indicates the number of times that OSPF failed to allocate buffers.
NumBufFreeFail	Indicates the number of times that OSPF failed to free buffers.
NumTxPkt	Indicates the number of packets transmitted by OSPF.
NumRxPkt	Indicates the number of packets received by OSPF.
NumTxDropPkt	Indicates the number of packets dropped before transmission by OSPF.
NumRxDropPkt	Indicates the number of packets dropped before reception by OSPF.
NumRxBadPkt	Indicates the number of packets received by OSPF that are bad.
NumSpfRun	Indicates the total number of SPF calculations performed by OSPF, which also includes the number of partial route table calculation for incremental updates.
LastSpfRun	Indicates the time (SysUpTime) since the last SPF calculated by OSPF.
LsdbTblSize	Indicates the number of entries in the link state database table.
NumAllocBdDDP	Indicates the number of times buffer descriptors were allocated for OSPF database description packets.
NumFreeBdDDP	Indicates the number of times buffer descriptors were freed after use as OSPF database description packets.
NumBadLsReq	Indicates the number of bad LSDB requests.
NumSeqMismatch	Indicates the number of mismatches for sequence numbers.
NumOspfRoutes	The count of OSPF routes.
NumOspfAreas	The count of OSPF areas.
NumOspfAdjacencies	The count of Adjacencies.

Viewing basic OSPF statistics for a port

Use statistics to help you monitor Open Shortest Path First (OSPF) performance. You can also use statistics in troubleshooting procedures.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View basic OSPF statistics:

   ```
   show ports statistics ospf main [{slot/port[/sub-port][-slot/port[/
   sub-port]][,...]}]
   ```

Example

View basic OSPF statistics:

```
Switch:1>enable
Switch:1#show ports statistics ospf main

================================================================================
                                Port Stats Ospf
================================================================================
PORT_NUM RX_HELLO   TX_HELLO   RXDB_DESCR TXDB_DESCR RXLS_UPDATE   TXLS_UPDATE
--------------------------------------------------------------------------------
1/3      0          0          0          0          0             0
```

Variable definitions

Use the data in the following table to use the **`show ports statistics ospf main`** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Job aid

The following table describes the output for the **`show ports statistics ospf main`** command.

Table 23: show ports statistics ospf main output description

Field	Description
PORT NUM	Indicates the port number.
RX_HELLO	Indicates the number of hello packets this interface receives.

Table continues…

Field	Description
TX_HELLO	Indicates the number of hello packets this interface transmitted.
RXDB_DESCR	Indicates the number of database descriptor packets this interface receives.
TXDB_DESCR	Indicates the number of database descriptor packets this interface transmitted.
RXLS_UPDATE	Indicates the number of link state update packets this interface receives.
TXLS_UPDATE	Indicates the number of link state update packets this interface transmitted.

Showing extended OSPF statistics

Use statistics to help you monitor Open Shortest Path First (OSPF) performance. You can also use statistics in troubleshooting procedures.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display extended OSPF information about the specified port or for all ports:

   ```
   show ports statistics ospf extended [{slot/port[/sub-port][-slot/
   port[/sub-port]][,...]}]
   ```

Example

Display extended OSPF information:

```
Switch:1>enable
Switch:1#show ports statistics ospf extended

================================================================================
                            Port Stats Ospf Extended
================================================================================
PORT_NUM RXLS_REQS  TXLS_REQS  RXLS_ACKS  TXLS_ACKS
--------------------------------------------------------------------------------
1/3      0          0          0          0
```

Variable definitions

Use the data in the following table to use the **show ports statistics ospf extended** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Job aid

The following table describes the output for the **show ports statistics ospf extended** command.

Table 24: show ports statistics ospf extended output description

Parameters	Description
PORT_NUM	Indicates the port number.
RXLS_REQS	Indicates the number of link state update request packets received by this interface.
TXLS_REQS	Indicates the number of link state request packets transmitted by this interface.
RXLS_ACKS	Indicates the number of link state acknowledge packets received by this interface.
TXLS_ACKS	Indicates the number of link state acknowledge packets transmitted by this interface.

Viewing ingress port-rate limit statistics

Use this procedure to view the ingress port-rate limit statistics. The system displays the statistics of the dropped packets and bytes.

This command is not available on all hardware platforms.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. View the ingress port-rate limit statistics:

   ```
   show interfaces gigabitethernet statistics rate—limiting [port
   {slot/port[/sub-port][-slot/port[/sub-port]][,...]}]
   ```

Example

```
Switch:1# show interfaces gigabitethernet statistics rate-limiting 1/1

================================================================================
                  QOS Interface Ingress Rate-Limiting Stats
================================================================================
PORT     DROPPING          DROPPING          DROPPING          DROPPING
         PKTS RATE         BYTES RATE        PKTS              BYTES
--------------------------------------------------------------------------------
1/1         9224                        9260507                  1430758
1436481032
```

Variable definitions

Use the data in the following table to use the `show qos rate—limiting` command.

Table 25: Variable definitions

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Viewing the management port statistics

Use this procedure to view the management port statistics.

This procedure only applies to hardware with a dedicated, physical management interface.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. View the management port statistics:

   ```
   show interfaces mgmtethernet statistics
   ```

Example

View management port statistics:

```
Switch:1#show interfaces mgmtethernet statistics
=============================================================================
                          Port Stats Interface
=============================================================================
PORT  IN        OUT                 IN                  OUT
NUM   OCTETS    OCTETS              PACKET              PACKET
-----------------------------------------------------------------------------
mgmt  7222116   44282               81789               586

PORT  IN        OUT                 IN                  OUT     OUTLOSS
NUM   FLOWCTRL  FLOWCTRL            PFC                 PFC     PACKETS
-----------------------------------------------------------------------------
mgmt   0         0                  0                   0       0
```

Clearing IPv6 statistics

Clear all IPv6 statistics if you do not require previous statistics.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Clear all the IPv6 statistics:

   ```
   clear ipv6 statistics all
   ```

3. Clear interface statistics:

   ```
   clear ipv6 statistics interface [general|icmp] [gigabitethernet
   <slot/port[/sub-port]>|mgmtethernet <slot/port[/sub-port]>|tunnel
   <1-2000> | vlan <1-4059>]
   ```

4. Clear TCP statistics:

   ```
   clear ipv6 statistics tcp
   ```

5. Enter the following command to clear UDP statistics:

   ```
   clear ipv6 statistics udp
   ```

Variable definitions

Use the information in the following table to use the **`clear ipv6 statistics`** command.

Variable	Value
vlan<*1-4059*>	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
gigabitethernet {slot/port[/sub-port]}	Identifies a single slot and port. If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
mgmtethernet {slot/port[/sub-port]}	Identifies the management port. This parameter only applies to hardware with a dedicated, physical management interface.
tunnel <*1-2000*>	Identifies a 6in4 tunnel ID.

Viewing ICMP statistics

View IPv6 ICMP statistics on an interface for ICMP messages sent over a particular interface.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View IPv6 ICMP statistics

   ```
   show ipv6 interface icmpstatistics [gigabitethernet <slot/port[/sub-
   port]>|mgmtethernet <slot/port[/sub-port]>|tunnel <1-2000> | vlan
   <1-4059>]
   ```

Example

View ICMP statistics:

```
Switch:1>show ipv6 interface icmpstatistics
================================================================================
                                    Icmp Stats
================================================================================

Icmp stats for IfIndex = 192

IcmpInMsgs: 0
IcmpInErrors: 0
IcmpInDestUnreachs : 0
IcmpInAdminProhibs : 0
IcmpInTimeExcds : 0
IcmpInParmProblems : 0
IcmpInPktTooBigs : 0
IcmpInEchos : 0
IcmpInEchoReplies : 0
IcmpInRouterSolicits : 0
IcmpInRouterAdverts : 0
InNeighborSolicits : 0
InNbrAdverts : 0
IcmpInRedirects : 0
IcmpInGroupMembQueries : 0
IcmpInGroupMembResponses : 0
```

Variable definitions

Use the data in the following table to use the **`show ipv6 interface icmpstatistics`** command

Variable	Value
<1-4059>	Shows ICMP statistics for the specific interface index. If you do not specify an interface index, the command output includes all IPv6 ICMP interfaces. Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
gigabitethernet {slot/port[/sub-port]}	Identifies a single slot and port. If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
mgmtethernet {slot/port[/sub-port]}	Identifies the management port. This parameter only applies to hardware with a dedicated, physical management interface.
tunnel *<1-2000>*	Identifies a 6in4 tunnel ID.

Viewing IPv6 DHCP Relay statistics

Display individual IPv6 DHCP Relay statistics for specific interfaces to manage network performance.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View statistics:

   ```
   show ipv6 dhcp-relay counters
   ```

   Note:

   Use the `sys action reset counters` command to clear DHCP Relay statistics.

Example

```
Switch:1#show ipv6 dhcp-relay counters

================================================================================
                               DHCPv6 Counters
================================================================================
INTERFACE                                REQUESTS   REPLIES
--------------------------------------------------------------------------------
1111:0:0:0:0:0:0:1111                    1          1
```

Job aid

The following table explains the output of the **`show ipv6 dhcp-relay counters`** command.

Table 26: show ipv6 dhcp-relay counters command output

Heading	Description
REQUESTS	Shows the number of DHCP and BootP requests on this interface.
REPLIES	Shows the number of DHCP and BootP replies on this interface.

Viewing IPv6 OSPF statistics

View OSPF statistics to analyze trends.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View statistics:

   ```
   show ipv6 ospf statistics
   ```

Example

View IPv6 OSPF statistics:

```
Switch:1>enable
Switch:1#show ipv6 ospf statistics

================================================================================
                                OSPFv3 Statistics
================================================================================
          NumTxPkt: 9958
          NumRxPkt: 8982
      NumTxDropPkt: 33
      NumRxDropPkt: 0
       NumRxBadPkt: 0
         NumSpfRun: 42
        LastSpfRun: 0 day(s), 02:44:32
       LsdbTblSize: 45
       NumBadLsReq: 0
    NumSeqMismatch: 0
NumOspfAdjacencies: 7
```

Job aid

The following table explains the output of the **`show ipv6 ospf statistics`** command.

Field	Description
NumTxPkt	Shows the count of sent packets.
NumRxPkt	Shows the count of received packets.
NumTxDropPkt	Shows the count of sent, dropped packets.
NumRxDropPkt	Shows the count of received, dropped packets.
NumRxBadPkt	Shows the count of received, bad packets.
NumSpfRun	Shows the count of intra-area route table updates with calculations using this area link-state database.
LastSpfRun	Shows the count of the most recent SPF run.
LsdbTblSize	Shows the size of the link-state database table.
NumBadLsReq	Shows the count of bad link requests.
NumSeqMismatch	Shows the count of sequence mismatched packets.

Viewing IPv6 statistics on an interface

View IPv6 statistics to view information about the IPv6 datagrams on an interface.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View statistics:

   ```
   show ipv6 interface statistics [gigabitethernet <slot/port[/sub-port]>|mgmtethernet <slot/port[/sub-port]>|tunnel <1-2000> | vlan <1-4059>]
   ```

Example

View IPv6 statistics on an interface:

```
Switch:1>enable
Switch:1#show ipv6 interface statistics

================================================================================
                                Interface Stats
================================================================================


If Stats for mgmt, IfIndex = 64

InReceives: 404
InHdrErrors: 0
InTooBigErrors : 0
InNoRoutes : 0
InAddrErrors : 0
InUnknownProtos : 0
InTruncatedPkts : 0
InDiscards : 0
InDelivers : 404
OutForwDatagrams : 0
OutRequests : 417
OutDiscards : 0
OutFragOKs : 0
OutFragFails : 0
OutFragCreates : 0

--More-- (q = quit)
```

Variable definitions

Use the data in the following table to use the **`show ipv6 interface statistics`** command

Variable	Value
vlan *<1-4059>*	Shows statistics for the specific interface index. If you do not specify an interface index, the command output includes all IPv6 interfaces. Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
gigabitethernet {slot/port[/sub-port]}	Identifies a single slot and port. If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
mgmtethernet {slot/port[/sub-port]}	Identifies the management port. This parameter only applies to hardware with a dedicated, physical management interface.
tunnel *<1-2000>*	Identifies a 6in4 tunnel ID.

Displaying IPsec statistics

Use the following procedure to clear Internet Protocol Security (IPsec) system statistics counters and display IPsec statistics on an interface. The device only clears system statistics counters on system reboot.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display statistics for IPsec for the system:

   ```
   show ipv6 ipsec statistics system
   ```

3. Display statistics for IPsec for an Ethernet interface:

   ```
   show ipv6 ipsec statistics gigabitethernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

4. Display statistics for IPsec for an VLAN interface:

   ```
   show ipv6 ipsec statistics vlan <1-4059>
   ```

5. Display statistics for IPsec on the management interface:

   Note:

   This step only applies to hardware with a dedicated, physical management interface.

   ```
   show ipv6 ipsec statistics mgmtethernet mgmt
   ```

6. Clear IPsec system statistics counters:

   ```
   clear ipsec stats all
   ```

Example

Display IPsec statistics for an Ethernet interface and a VLAN interface:

```
Switch:1>enable
Switch:1(config)#show ipv6 ipsec statistics system

================================================================================
                            IPSEC Global Statistics
================================================================================
InSuccesses           = 0
InSPViolations        = 0
InNotEnoughMemories   = 0
InAHESPReplays        = 0
InAHFailures          = 0
InESPFailures         = 0
OutSuccesses          = 0
OutSPViolations       = 0
OutNotEnoughMemories  = 0
generalError          = 0
InAHSuccesses         = 0
InESPSuccesses        = 0
OutAHSuccesses        = 0
```

```
OutESPSuccesses      = 0
OutKBytes            = 0
OutBytes             = 0
InKBytes             = 0
InBytes              = 0
TotalPacketsProcessed= 0

TotalPacketsByPassed = 285984828
OutAHFailures        = 167772160
OutESPFailures       = 167772160
InMD5Hmacs           = 167772160
InSHA1Hmacs          = 167772160
InAESXCBCs           = 167772160
InAnyNullAuth        = 167772160
In3DESCBCs           = 167772160
InAESCBCs            = 167772160
InAESCTRs            = 167772160
InAnyNullEncrypt     = 167772160
OutMD5Hmacs          = 167772160
OutSHA1Hmacs         = 167772160
OutAESXCBCs          = 167772160
OutInAnyNullAuth     = 167772160
Out3DESCBCs          = 167772160
OutAESCBCs           = 167772160
OutAESCTRs           = 167772160
OutInAnyNullEncrypt  = 167772160

Switch:1(config)#show ipv6 ipsec statistics gigabitethernet 1/13

================================================================================
                              Ipsec  Port  Stats
================================================================================
Ifindex              = 204
InSuccesses          = 0
InSPViolations       = 0
InNotEnoughMemories  = 0
InAHESPReplays       = 0
InAHFailures         = 0
InESPFailures        = 0
OutSuccesses         = 0
OutSPViolations      = 0
OutNotEnoughMemories = 0
generalError         = 0

Switch:1(config)#show ipv6 ipsec statistics vlan 1

================================================================================
                               Ipsec  Vlan  Stats
================================================================================
Ifindex              = 2049
InSuccesses          = 0
InSPViolations       = 0
InNotEnoughMemories  = 0
InAHESPReplays       = 0
InAHFailures         = 0
InESPFailures        = 0
OutSuccesses         = 0
OutSPViolations      = 0
OutNotEnoughMemories = 0
generalError         = 0
```

```
Switch:1#show ipv6 ipsec statistics mgmtethernet mgmt

================================================================================
                              Ipsec  Port  Stats
```

```
================================================================================
Ifindex              = 64
InSuccesses          = 0
InSPViolations       = 0
InNotEnoughMemories  = 0
InAHESPReplays       = 0
InESPReplays         = 0
InAHFailures         = 0
InESPFailures        = 0
OutSuccesses         = 0
OutSPViolations      = 0
OutNotEnoughMemories = 0
generalError         = 0
```

Variable definitions

Use the data in the following table to use the **show ipsec statistics** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
mgmtethernet mgmt	Identifies the interface as the management interface.
vlan <*1-4059*>	Specifies the VLAN.

Job aid

The following table describes the fields in the output for the **show ipv6 ipsec statistics system** command.

Parameter	Description
InSuccesses	Specifies the number of ingress packets IPsec successfully carries.
InSPViolations	Specifies the number of ingress packets IPsec discards since boot time because of a security policy violation.
InNotEnoughMemories	Specifies the number of ingress packets IPsec discards since boot time because not enough memory is available.
InAHESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the encapsulating security payload (ESP) replay check fails.
InAHFailures	Specifies the number of ingress packets IPsec discards since boot time because the AH authentication check fails.

Table continues…

Parameter	Description
InESPFailures	Specifies the number of ingress packets IPsec discards since boot time because the ESP authentication check fails.
OutSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutSPViolations	Specifies the number of egress packets IPsec discards since boot time because a security policy violation occurs.
OutNotEnoughMemories	Specifies the number of egress packets IPsec discards since boot time because not enough memory is available since boot time.
generalError	Specifies a general error.
InAHSuccesses	Specifies the number of ingress packets IPsec carries because the AH authentication succeeds.
InESPSuccesses	Specifies the number of ingress packets IPsec carries since boot time because the ESP authentication succeeds.
OutAHSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutESPSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutKBytes	Specifies the total number of kilobytes on egress.
OutBytes	Specifies the total number of bytes on egress.
InKBytes	Specifies the total number of bytes on ingress.
InBytes	Specifies the total number of bytes on ingress.
TotalPacketsProcessed	Specifies the total number of packets processed.
TotalPacketsByPassed	Specifies the total number of packets bypassed.
OutAHFailures	Specifies the number of egress packets IPsec discards since boot time because the AH authentication check fails.
OutESPFailures	Specifies the number of egress packets IPsec discards since boot time because the ESP authentication check fails.
InMD5Hmacs	Specifies the number of inbound HMAC MD5 occurrences since boot time.
InSHA1Hmacs	Specifies the number of inbound HMAC SHA1 occurrences since boot time.
InAESXCBCs	Specifies the number of inbound AES XCBC MAC occurrences since boot time.

Table continues…

Parameter	Description
InAnyNullAuth	Specifies the number of inbound null authentication occurrences since boot time.
In3DESCBCs	Specifies the number of inbound 3DES CBC occurrences since boot time.
InAESCBCs	Specifies the number of inbound AES CBC occurrences since boot time.
InAESCTRs	Specifies the number of inbound AES CTR occurrences since boot time.
InAnyNullEncrypt	Specifies the number of inbound null occurrences since boot time. Used for debugging purposes.
OutMD5Hmacs	Specifies the number of outbound HMAC MD5 occurrences since boot time.
OutSHA1Hmacs	Specifies the number of outbound HMAC SHA1 occurrences since boot time.
OutAESXCBCs	Specifies the number of outbound AES XCBC MAC occurrences since boot time.
OutInAnyNullAuth	Specifies the number of outbound null authentication occurrences since boot time.
Out3DESCBCs	Specifies the number of outbound 3DES CBC occurrences since boot time.
OutAESCBCs	Specifies the number of outbound AES CBC occurrences since boot time.
OutAESCTRs	Specifies the number of outbound AES CTR occurrences since boot time.
OutInAnyNullEncrypt	Specifies the number of outbound null occurrences since boot time. Used for debugging purposes.

The following table describes the fields in the output for the **`show ipv6 ipsec statistics gigabitethernet {slot/port[-slot/port][,...]}`** command.

Parameter	Description
Ifindex	Specifies the interface.
InSuccesses	Specifies the number of ingress packets IPsec successfully carries.
InSPViolations	Specifies the number of ingress packets IPsec discards since boot time because of a security policy violation.
InNotEnoughMemories	Specifies the number of ingress packets IPsec discards since boot time because not enough memory is available.

Table continues…

Parameter	Description
InAHESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the encapsulating security payload (ESP) replay check fails.
InAHFailures	Specifies the number of ingress packets IPsec discards since boot time because the AH authentication check fails.
InESPFailures	Specifies the number of ingress packets IPsec discards since boot time because the ESP authentication check fails.
OutSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutSPViolations	Specifies the number of egress packets IPsec discards since boot time because a security policy violation occurs.
OutNotEnoughMemories	Specifies the number of egress packets IPsec discards since boot time because not enough memory is available since boot time.
generalError	Specifies a general error.

The following table describes the fields in the output for the **`show ipv6 ipsec statistics vlan <1–4059>`** command.

Parameter	Description
Ifindex	Specifies the interface.
InSuccesses	Specifies the number of ingress packets IPsec successfully carries.
InSPViolations	Specifies the number of ingress packets IPsec discards since boot time because of a security policy violation.
InNotEnoughMemories	Specifies the number of ingress packets IPsec discards since boot time because not enough memory is available.
InAHESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the encapsulating security payload (ESP) replay check fails.
InAHFailures	Specifies the number of ingress packets IPsec discards since boot time because the AH authentication check fails.
InESPFailures	Specifies the number of ingress packets IPsec discards since boot time because the ESP authentication check fails.
OutSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.

Table continues…

Parameter	Description
OutSPViolations	Specifies the number of egress packets IPsec discards since boot time because a security policy violation occurs.
OutNotEnoughMemories	Specifies the number of egress packets IPsec discards since boot time because not enough memory is available since boot time.
generalError	Specifies a general error.

The following table describes the fields in the output for the **`show ipv6 ipsec statistics mgmtethernet mgmt`** command.

Parameter	Description
Ifindex	Specifies the interface.
InSuccesses	Specifies the number of ingress packets IPsec successfully carries.
InSPViolations	Specifies the number of ingress packets IPsec discards since boot time because of a security policy violation.
InNotEnoughMemories	Specifies the number of ingress packets IPsec discards since boot time because not enough memory is available.
InAHESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the AH replay check fails.
InESPReplays	Specifies the total number of ingress packets IPsec discards since boot time because the encapsulating security payload (ESP) replay check fails.
InAHFailures	Specifies the number of ingress packets IPsec discards since boot time because the AH authentication check fails.
InESPFailures	Specifies the number of ingress packets IPsec discards since boot time because the ESP authentication check fails.
OutSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutSPViolations	Specifies the number of egress packets IPsec discards since boot time because a security policy violation occurs.
OutNotEnoughMemories	Specifies the number of egress packets IPsec discards since boot time because not enough memory is available since boot time.
generalError	Specifies a general error.

Viewing IPv6 VRRP statistics

View IPv6 VRRP statistics to monitor network performance

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View statistics for the device and for all interfaces:

   ```
   show ipv6 vrrp statistics [link-local WORD<0-127>]] [vrid <1-255>]
   ```

Example

View IPv6 VRRP statistics for VRID 1.

```
Switch:1(config)#show ipv6 vrrp statistics vrid 1

================================================================================
                      VRRP Interface Stats - GlobalRouter
================================================================================

VRID  P/V   BECOME_MASTER ADVERTISE_RCV
--------------------------------------------------------------------------------
1     84    2             17372
1     85    2             17372
1     86    1             0
1     87    1             0
1     1001  2             17372

VRID  P/V   ADVERTISE_INT_ERR TTL_ERR       PRIO_0_RCV
--------------------------------------------------------------------------------
1     84    0                 0             0
1     85    0                 0             0
1     86    0                 0             0
1     87    0                 0             0
1     1001  0                 0             0

VRID  P/V   PRIO_0_SENT   INVALID_TYPE_ERR ADDRESS_LIST_ERR UNKNOWN_AUTHTYPE
--------------------------------------------------------------------------------

--More-- (q = quit)
```

Variable definitions

Use the data in the following table to use the **`show ipv6 vrrp statistics`** command.

Variable	Value
link-local *WORD<0–127>*	Shows statistics for a specific link-local address.
vrid *<1–255>*	Shows statistics for a specific VRID.

Job aid

The following table describes the output for the **`show ipv6 vrrp statistics`** command.

Table 27: show ipv6 vrrp statistics command output

Heading	Description
CHK_SUM_ERR	Shows the number of VRRP packets received with an invalid VRRP checksum value.
VERSION_ERR	Shows the number of VRRP packets received with an unknown or unsupported version number.
VRID_ERR	Shows the number of VRRP packets received with an invalid VrID for this virtual router.
BECOME_MASTER	Shows the total number of times that the state of this virtual router has transitioned to master. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
ADVERTISE_RCV	Shows the total number of VRRP advertisements received by this virtual router. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
ADVERTISE_INT_ERR	Shows the total number of VRRP advertisement packets received for which the advertisement interval is different than the one configured for the local virtual router. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
TTL_ERR	Shows the total number of VRRP packets received by the virtual router with IPv4 TTL (for VRRP over IPv4) or IPv6 Hop Limit (for VRRP over IPv6) not equal to 255. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
PRIO_0_RCV	Shows the total number of VRRP packets received by the virtual router with a priority of 0. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
PRIO_0_SENT	Shows the total number of VRRP packets sent by the virtual router with a priority of 0. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.

Table continues…

Heading	Description
INVALID_TYPE_ERR	Shows the number of VRRP packets received by the virtual router with an invalid value in the 'type' field. Discontinuities in the value of this counter can occur at reinitialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
ADDRESS_LIST_ERR	Shows the total number of packets received for which the address list does not match the locally configured list for the virtual router. Discontinuities in the value of this counter can occur at reinitialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
UNKNOWN_AUTHTYPE	Shows the total number of packets received with an unknown authentication type.
PACKLEN_ERR	Shows the total number of packets received with a packet length less than the length of the VRRP header. Discontinuities in the value of this counter can occur at reinitialization of the management system, and at other times as indicated by the value of DiscontinuityTime.

Showing the EAPoL status of the device

Display the current device configuration.

Note:

Use the **clear-stats** command to clear EAP or NEAP statistics.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the current device configuration by using the following command:

   ```
   show eapol system
   ```

Example

```
Switch:1#show eapol system
================================================================================
                                  Eapol System
================================================================================
                      eap : enabled
          non-eap-pwd-fmt : ip-addr.mac-addr.port-number
      non-eap-pwd-fmt key :
  non-eap-pwd-fmt padding : disabled
--------------------------------------------------------------------------------
```

Showing EAPoL authenticator statistics

Display the authenticator statistics to manage network performance.

Note:

Use the **clear-stats** command to clear EAP or NEAP statistics.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the authenticator statistics:

```
show eapol auth-stats interface [gigabitEthernet [{slot/port[/sub-port][-slot/port[/sub-port]][,...]}]]
```

Example

Note:

Slot and port information can differ depending on hardware platform.

```
Switch:1#show eapol auth-stats interface
```

```
================================================================================
                          Eap Authenticator Statistics
================================================================================
PORT   EAP    AUTH-EAP    START LOGOFF INVALID LENGTH LAST-RX    LAST-RX
       RCVD   TX          RCVD  RCVD   FRAMES  ERROR  VER        SRC
--------------------------------------------------------------------------------
1/1    716    1074        0     0      0       0      1          18:a9:05:b1:04:ce
1/2    0      0           0     0      0       0      0          00:00:00:00:00:00
1/3    0      0           0     0      0       0      0          00:00:00:00:00:00
1/4    0      5           0     0      0       0      0          00:00:00:00:00:00
1/5    0      0           0     0      0       0      0          00:00:00:00:00:00
1/6    0      0           0     0      0       0      0          00:00:00:00:00:00
1/7    0      0           0     0      0       0      0          00:00:00:00:00:00
1/8    0      0           0     0      0       0      0          00:00:00:00:00:00
1/9    0      0           0     0      0       0      0          00:00:00:00:00:00
1/10   0      0           0     0      0       0      0          00:00:00:00:00:00
--More-- (q = quit)
```

Variable definitions

Use the data in the following table to use the **show eapol auth-stats interface** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Job aid

The following table describes the output for the **show eapol auth-stats interface** command.

Table 28: show eapol auth-stats interface field descriptions

Parameter	Description
PORT	Displays the port number in use.
EAP RCVD	Displays the number of EAPoL-EAP frames received by this Authenticator.
AUTH-EAP TX	Displays the number of EAPoL-EAP frames transmitted by the Authenticator.
START RCVD	Displays the number of EAPoL start frames received by this Authenticator.
LOGOFF RCVD	Displays the number of EAPoL logoff frames received by this Authenticator.
INVALID FRAMES	Displays the number of EAPoL frames received by this Authenticator in which the frame type is not recognized.
LENGTH ERROR	Displays the number of EAPoL frames received by this Authenticator in which the Packet Body Length field is invalid.
LAST-RX VER	Displays the last received version of the EAPoL frame by this Authenticator.
LAST-RX SRC	Displays the source MAC address of the last received EAPoL frame by this Authenticator.

Viewing EAPoL session statistics

View EAPoL session statistics to manage network performance.

Note:

Use the **clear-stats** command to clear EAP/NEAP statistics.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the session statistics:

```
show eapol session—stats interface [gigabitEthernet [{slot/port[/
sub-port][-slot/port[/sub-port]][,...]}]
```

Example

```
Switch:1#show eapol session-stats interface
================================================================================
                      Eap Authenticator Session Statistics
================================================================================
```

```
PORT  MAC     SESSION   AUTHENTIC       SESSION          TERMINATE       USER
NUM           ID        METHOD          TIME             CAUSE           NAME
-------------------------------------------------------------------------------
1/1   18:a9:05:b1:04:ce    cb000000  remote-server   0 day(s), 05:58:16    not-terminated
sachin
1/4   00:00:00:00:00:01    cb000002  remote-server   0 day(s), 05:48:01    not-terminated
000000000001
-------------------------------------------------------------------------------
```

Variable definitions

Use the data in the following table to use the **show eapol session-stats interface** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Job aid

The following table describes the output for the **show eapol session-stats interface** command.

Table 29: show eapol session-stats interface field descriptions

Parameter	Description
PORT NUM	Displays the port number in use.
MAC	Displays the MAC address of the client.
USER NAME	Displays the user name of the Supplicant Authenticator Port Access Entity (PAE).
SESSION ID	Displays a unique identifier for the session.
AUTHENTIC METHOD	Displays the authentication method (remote or local RADIUS server) used to establish the session.
SESSION TIME	Displays the duration of the session (in seconds).
TERMINATE CAUSE	Displays the reason the session terminated.

Viewing non-EAPoL MAC information

Use this procedure to view non-EAPoL client MAC information on a port.

Note:

Use the **clear-stats** command to clear EAP/NEAP statistics.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the non-EAPoL MAC information:

   ```
   show eapol multihost non-eap-mac status [vlan <1-4059>][{slot/port[/
   sub-port][-slot/port[/sub-port]][,...]}]
   ```

Example

```
Switch:1#show eapol multihost non-eap-mac status
================================================================================
                              Non-Eap Oper Status
================================================================================
PORT  MAC                 STATE             VLAN
NUM                                         ID
--------------------------------------------------------------------------------
1/3 00:00:00:11:22:33 RADIUS-Authenticated    250
--------------------------------------------------------------------------------
```

Variable definitions

Use the data in the following table to use the **show eapol multihost non-eap-mac status** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

Job aid

The following table describes the output for the **show eapol multihost non-eap-mac status** command.

Table 30: show eapol multihost non-eap-mac status field descriptions

Parameter	Description
PORT NUM	Displays the port number in use.
MAC	Displays the MAC address of the client.
STATE	Indicates the authentication status of the non EAP host that is authenticated using radius server.
VLAN ID	Indicates the VLAN assigned to the client.

Viewing port EAPoL operation statistics

Use this procedure to view port EAPoL operation statistics.

Note:

Use the **clear-stats** command to clear EAP/NEAP statistics.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the port EAPoL operation statistics information:

   ```
   show eapol status interface [gigabitEthernet [{slot/port[/sub-port]
   [-slot/port[/sub-port]][,...]}] [vlan <1-4059>]
   ```

Example

```
Switch:1#show eapol status interface
================================================================================
                                Eap Oper Stats
================================================================================
PORT  MAC                 PAE               VLAN
NUM                       STATUS            ID
--------------------------------------------------------------------------------
1/1   18:a9:05:b1:04:ce   authenticated     10
--------------------------------------------------------------------------------
Total Number of EAP sessions : 1
```

Variable definitions

Use the data in the following table to use the **show eapol status** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
<1-4059>	Specifies the VLAN ID for which to show the statistics.

Job aid

The following table describes the output for the **show eapol status interface** command.

Table 31: show eapol status interface field descriptions

Parameter	Description
PORT NUM	Displays the port number in use.
MAC	Displays the MAC address of the client.

Table continues…

Parameter	Description
PAE STATUS	Indicates the current state of the authenticator PAE state machine.
VLAN ID	Indicates the VLAN assigned to the client.

Viewing IP multicast threshold exceeded statistics

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View statistics:

   ```
   show sys stats ipmc-threshold-exceeded-cnt
   ```

Example

```
Switch:1#show sys stats ipmc-threshold-exceeded-cnt
            SourceGroupThresholdExceeded : 7372
            EgressStreamThresholdExceeded : 7331
```

Viewing statistics using EDM

Use statistics to help monitor the performance of the switch.

About this task

To reset all statistics counters, click **Clear Counters**. After you click this button, all Cumulative, Average, Minimum, Maximum, and LastVal columns reset to zero, and automatically begin to recalculate statistical data.

Important:

The **Clear Counters** function does not affect the AbsoluteValue counter for the device. The **Clear Counters** function clears all cached data in EDM except AbsoluteValue. Perform the following steps to reset AbsoluteValues.

Procedure

1. In the Device Physical View tab, select the Device.
2. In the navigation tree, expand the following folders: **Configuration** > **Edit**.
3. Click **Chassis**.
4. Click the **System** tab.
5. In ActionGroup1, select **resetCounters**, and then click **Apply**.

Graphing chassis statistics

Create graphs of chassis statistics to generate a visual representation of your data.

Procedure

1. In the Device Physical View, select the chassis.
2. In the navigation tree, expand the following folders: **Configuration** > **Graph**.
3. Click **Chassis**.
4. On the Graph Chassis tab, select the tab with the data you want to graph:
   - System
   - SNMP
   - IP
   - ICMP In
   - ICMP Out
   - TCP
   - UDP
5. Select the statistic you want to graph.
6. Select the graph type:
   - line chart
   - area chart
   - bar chart
   - pie chart

Graphing port statistics

You can create graphs for many port statistics to generate a visual representation of your data.

Procedure

1. In the Device Physical View, select the port or ports for which you want to create a graph.
2. Perform the following steps:
   - Right-click a port or multiple ports. On the shortcut menu, choose **Graph**.
   - In the navigation tree, expand the following folders: **Configuration** > **Graph**, and then click **Port**.
3. When the graph port dialog box appears, click the tab for which you want to graph the statistics.

4. Select the item for which you want to graph the statistics.
5. Select a graph type:
   - bar
   - pie
   - chart
   - line

Viewing chassis system statistics

Use the following procedure to create graphs for chassis statistics.

Procedure

1. In the Device Physical View, select the chassis.
2. In the navigation tree, expand the following folders: **Configuration** > **Graph**.
3. Click **Chassis**.
4. Click the **System** tab.

System field descriptions

The following table describes the fields on the System tab.

Name	Description
MenUsed	The percentage of memory space used. Only the AbsoluteValue column is valid in the System tab. All other columns display as N/A because they are percentages and not actual memory counters.
MemFree	The amount in kilobytes of free memory.
CpuCurrentUtil	Percentage of CPU utilization.

Viewing chassis SNMP statistics

View chassis SNMP statistics to monitor network performance.

Procedure

1. In the Device Physical View, select the chassis.
2. In the navigation tree, expand the following folders: **Configuration** > **Graph**.
3. Click **Chassis**.
4. Click the **SNMP** tab.

SNMP field descriptions

The following table describes parameters on the **SNMP** tab.

Name	Description
InPkts	The number of messages delivered to the SNMP entity from the transport service.
OutPkts	The number of SNMP messages passed from the SNMP protocol entity to the transport service.
InTotalReqVars	The number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
InTotalSetVars	The number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
InGetRequests	The number of SNMP Get-Request PDUs the SNMP protocol accepts and processes.
InGetNexts	The number of SNMP Get-Next PDUs the SNMP protocol accepts and processes.
InSetRequests	The number of SNMP Set-Request PDUs the SNMP protocol accepts and processes.
InGetResponses	The number of SNMP Get-Response PDUs the SNMP protocol accepts and processes.
OutTraps	The number of SNMP Trap PDUs the SNMP protocol generates.
OutTooBigs	The number of SNMP PDUs the SNMP protocol generates for which the value of the error-status field is tooBig.
OutNoSuchNames	The number of SNMP PDUs the SNMP protocol generates for which the value of the error-status field is noSuchName.
OutBadValues	The number of SNMP PDUs the SNMP protocol generates for which the value of the error-status field is badValue.
OutGenErrs	The number of SNMP PDUs the SNMP protocol generates for which the value of the error-status field is genErr.
InBadVersions	The number of SNMP messages delivered to the SNMP protocol entity for an unsupported SNMP version.
InBadCommunityNames	The number of SNMP messages delivered to the SNMP protocol entity that used an SNMP community name not known to said entity.
InBadCommunityUses	The number of SNMP messages delivered to the SNMP protocol entity that represented an SNMP operation not allowed by the SNMP community named in the message.
InASNParseErrs	The number of ASN.1 or BER errors the SNMP protocol encountered when decoding received SNMP messages.
InTooBigs	The number of SNMP PDUs delivered to the SNMP protocol entity for which the value of the error-status field is tooBig.

Table continues…

Name	Description
InNoSuchNames	The number of SNMP PDUs delivered to the SNMP protocol entity for which the value of the error-status field is noSuchName.
InBadValues	The number of SNMP PDUs delivered to the SNMP protocol entity for which the value of the error-status field is badValue.
InReadOnlys	The number of SNMP PDUs delivered to the SNMP protocol entity for which the value of the error-status field is readOnly. It is a protocol error to generate an SNMP PDU containing the value "readOnly" in the error-status field. This object is provided to detect incorrect implementations of the SNMP.
InGenErrs	The number of SNMP PDUs delivered to the SNMP protocol entity for which the value of the error-status field is genErr.

Viewing chassis IP statistics

View chassis IP statistics to monitor network performance.

Procedure

1. In the Device Physical View, select the chassis.
2. In the navigation tree, expand the following folders: **Configuration** > **Graph**.
3. Click **Chassis**.
4. Click the **IP** tab.

IP field descriptions

The following table describes parameters on the **IP** tab.

Name	Description
InReceives	The number of input datagrams received from interfaces, including those received in error.
InHdrErrors	The number of input datagrams discarded due to errors in the IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options.
InAddrErrors	The number of input datagrams discarded because the IP address in the IP header destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities that are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities that do not act as IP

Table continues…

Name	Description
	Gateways, this counter includes only those packets that were Source-Routed by way of this entity and had successful Source-Route option processing.
InUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing but that were discarded (for example, for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.
InDelivers	The number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	The number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in ipForwDatagrams.
OutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that were discarded (for example, for lack of buffer space). This counter includes datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
OutNoRoutes	The number of IP datagrams discarded because no route was found to transmit them to their destination. This counter includes any packets counted in ipForwDatagrams that meet this no-route criterion. This counter includes any datagrams a host cannot route because all default gateways are down.
FragOKs	The number of IP datagrams that were successfully fragmented at this entity.
FragFails	The number of IP datagrams that were discarded because they needed to be fragmented at this entity but cannot be, for example, because the Don't Fragment flags were set.
FragCreates	The number of IP datagram fragments that were generated as a result of fragmentation at this entity.
ReasmReqds	The number of IP fragments received that needed to be reassembled at this entity.
ReasmOKs	The number of IP datagrams successfully reassembled.
ReasmFails	The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so on). This number is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.

Viewing chassis ICMP In statistics

View chassis ICMP In statistics to monitor network performance.

Procedure

1. In the Device Physical View, select the chassis.
2. In the navigation tree, expand the following folders: **Configuration** > **Graph**.
3. Click **Chassis**.
4. Click the **ICMP In** tab.

ICMP In field descriptions

The following table describes parameters on the **ICMP In** tab.

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

Viewing chassis ICMP Out statistics

View chassis ICMP Out statistics to monitor network performance.

Procedure

1. In the Device Physical View, select the chassis.
2. In the navigation tree, expand the following folders: **Configuration** > **Graph**.
3. Click **Chassis**.
4. Click the **ICMP Out** tab.

ICMP Out field descriptions

The following table describes parameters on the **ICMP Out** tab.

Name	Description
SrcQuenchs	The number of ICMP Source Quench messages sent.

Table continues…

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

Viewing chassis TCP statistics

View TCP statistics to monitor network performance.

Procedure

1. In the Device Physical View, select the chassis.
2. In the navigation tree, expand the following folders: **Configuration** > **Graph**.
3. Click **Chassis**.
4. Click the **TCP** tab.

TCP field descriptions

The following table describes parameters on the **TCP** tab.

Name	Description
ActiveOpens	The number of times TCP connections made a direct transition to the SYN-SENT state from the CLOSED state.
PassiveOpens	The number of times TCP connections made a direct transition to the SYN-RCVD state from the LISTEN state.
AttemptFails	The number of times TCP connections made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections made a direct transition to the LISTEN state from the SYN-RCVD state.
EstabResets	The number of times TCP connections made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.

Table continues…

Name	Description
CurrEstab	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
InSegs	The number of segments received, including those received in error. This count includes segments received on currently established connections.
OutSegs	The number of segments sent, including those on current connections, but excluding those containing only retransmitted octets.
RetransSegs	The number of segments retransmitted that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
InErrs	The number of segments received in error (for example, bad TCP checksums).
OutRsts	The number of TCP segments sent containing the RST flag.
HCInSegs	The number of segments received, including those received in error. This count includes segments received on currently established connections. This object is the 64-bit equivalent of InSegs.
HCOutSegs	The number of segments sent, including those on current connections, but excluding those containing only retransmitted octets. This object is the 64-bit equivalent of OutSegs.

Viewing chassis UDP statistics

Display User Datagram Protocol (UDP) statistics to see information about the UDP datagrams.

Procedure

1. In the Device Physical View, select the chassis.
2. In the navigation tree, expand the following folders: **Configuration** > **Graph**.
3. Click **Chassis**.
4. Click the **UDP** tab.
5. Select the information you want to graph.
6. Select the type of graph you want:
   - line
   - area
   - bar
   - pie
7. To clear counters, click **Clear Counters**. Discontinuities in the value of these counters can occur when the management system reinitializes, and at other times as indicated by discontinuities in the value of sysUpTime.

UDP field descriptions

Use the data in the following table to use the **UDP** tab.

Name	Description
NoPorts	The number of received UDP datagrams with no application at the destination port. 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.
InErrors	The number of received UDP datagrams that were not delivered for reasons other than the lack of an application at the destination port. 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.
InDatagrams	The number of UDP datagrams delivered to UDP users, for devices that can receive more than 1 000 000 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.
OutDatagrams	The number of UDP datagrams sent from this entity. 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.
HCInDatagrams	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
HCOutDatagrams	The number of UDP datagrams sent from this entity, for devices that can transmit more than 1 million UDP datagrams for each second. Discontinuities in the value of this counter can occur at reinitialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime.

Viewing port interface statistics

View port interface statistics to manage network performance.

Procedure

1. In the Device Physical View, select a port.
2. In the navigation tree, expand the following folders: **Configuration** > **Graph**.
3. Click **Port**.
4. Click the **Interface** tab.

Interface field descriptions

The following table describes parameters on the **Interface** tab.

Name	Description
InOctets	Specifies the number of octets received on the interface, including framing characters.
OutOctets	Specifies the number of octets transmitted from the interface, including framing characters.
InUcastPkts	Specifies the number of packets delivered by this sublayer to a higher sublayer that were not addressed to a multicast or broadcast address at this sublayer.
OutUcastPkts	Specifies the number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast address at this sublayer. The total number includes those packets discarded or not sent.
InMulticastPkts	Specifies the number of packets delivered by this sublayer to a higher sublayer that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both group and functional addresses.
OutMulticastPkts	Specifies the number of packets that higher-level protocols requested be transmitted, and that are addressed to a multicast address at this sublayer, including those that were discarded or not sent. For a MAC layer protocol, this number includes both group and functional addresses.
InBroadcastPkts	Specifies the number of packets delivered by this sublayer to a higher sublayer that are addressed to a broadcast address at this sublayer.
OutBroadcastPkts	Specifies the number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this sublayer, including those that were discarded or not sent.
InDiscards	Specifies the number of inbound packets that are discarded because of frames with errors or invalid frames or, in some cases, to fill up buffer space.
InErrors	For packet-oriented interfaces, specifies 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.
InUnknownProtos	For packet-oriented interfaces, specifies 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 were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter is always 0.
HCInPfcPkts	Specifies the total number of Priority Flow Control (PFC) packets received by this interface. This number does not increment for port-level flow control.

Table continues…

Name	Description
HCOutPfcPkts	Specifies the total number of PFC packets transmitted by this interface. This number does not increment for port-level flow control.
InFlowCtrlPkts	Specifies the number of port-level flow control packets received by this interface.
OutFlowCtrlPkts	Specifies the number of port-level flow control packets transmitted by this interface.
InPfcPkts	Specifies the total number of port-level flow control packets received by this interface.
OutPfcPkts	Specifies the total number of port-level flow control packets transmitted by this interface.
NumStateTransition	Specifies the number of times the port went in and out of service; the number of state transitions from up to down.

Viewing port Ethernet errors statistics

View port Ethernet errors statistics to manage network performance.

Procedure

1. In the Device Physical View, select a port.
2. In the navigation tree, expand the following folders: **Configuration** > **Graph**.
3. Click **Port**.
4. Click the **Ethernet Errors** tab.

Ethernet Errors field descriptions

The following table describes parameters on the **Ethernet Errors** tab.

Name	Description
AlignmentErrors	Specifies a count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object increments when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
FCSErrors	Specifies a count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object increments when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3

Table continues…

Name	Description
	Layer Management, counted exclusively according to the error status presented to the LLC.
InternalMacTransmitErrors	Specifies a count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object. 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 transmission errors on a particular interface that are not otherwise counted.
InternalMacReceiveErrors	Specifies a count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object. The precise meaning of the count represented by an instance of this object is implementation-specific. In particular, an instance of this object can represent a count of receive errors on a particular interface that are not otherwise counted.
CarrierSenseErrors	Specifies the number of times that the carrier sense condition is lost or not asserted when the switch attempts to transmit a frame on a particular interface. The count represented by an instance of this object increments at most once for each transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
FrameTooLongs	Specifies a count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object increments when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
SQETestErrors	Specifies a count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation described in section 7.2.4.6 of the same document.
DeferredTransmissions	Specifies a count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollisionFrames	Specifies a count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by

Table continues…

Name	Description
	the corresponding instance of either the UcastPkts, MulticastPkts, or BroadcastPkts objects and is not counted by the corresponding instance of the MultipleCollisionFrames object.
MultipleCollisionFrames	Specifies a count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the UcastPkts, MulticastPkts, or BroadcastPkts objects and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	Specifies the number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet; 512 corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
ExcessiveCollisions	Specifies a count of frames for which transmission on a particular interface fails due to excessive collisions.
FrameTooShorts	Specifies the number of frames, encountered on this interface, that are too short.
LinkFailures	Specifies the number of link failures encountered on this interface.
PacketErrors	Specifies the number of packet errors encountered on this interface.
CarrierErrors	Specifies the number of carrier errors encountered on this interface.
LinkInactiveErrors	Specifies the number of link inactive errors encountered on this interface.

Viewing port bridging statistics

View port bridging errors statistics to manage network performance.

This tab does not appear for all hardware models.

Procedure

1. In the Device Physical View, select a port.
2. In the navigation pane, expand the following folders: **Configuration** > **Graph**.
3. Click **Port**.
4. Click the **Bridging** tab.

Bridging field descriptions

The following table describes parameters on the Bridging tab.

Name	Description
InUnicastFrames	Shows the number of incoming unicast frames bridged.
InMulticastFrames	Shows the number of incoming multicast frames bridged.
InBroadcastFrames	Shows the number of incoming broadcast frames bridged.
InDiscards	Shows the number of frames discarded by the bridging entity.
OutFrames	Shows the number of outgoing frames bridged.

Viewing port spanning tree statistics

View port spanning tree statistics to manage network performance.

Procedure

1. In the Device Physical View, select a port.
2. In the navigation tree, expand the following folders: **Configuration** > **Graph**.
3. Click **Port**.
4. Click the **Spanning Tree** tab.

Spanning Tree field descriptions

The following table describes parameters on the **Spanning Tree** tab.

Name	Description
InConfigBpdus	The number of Config BPDUs received.
InTcnBpdus	The number of Topology Change Notifications BPDUs received.
InBadBpdus	The number of unknown or malformed BPDUs received.
OutConfigBpdus	The number of Config BPDUs transmitted.
OutTcnBpdus	The number of Topology Change Notifications BPDUs transmitted.

Viewing port routing statistics

View port routing statistics to manage network performance.

This tab does not appear for all hardware models.

Procedure

1. In the Device Physical View, select a port.
2. In the navigation pane, expand the following folders: **Configuration** > **Graph**.
3. Click **Port**.
4. Click the **Routing** tab.

Routing field descriptions

Use the data in the following table to use the Routing tab.

Name	Description
InUnicastFrames	Shows the number of incoming unicast frames routed.
InMulticastFrames	Shows the number of incoming multicast frames routed.
InDiscards	Shows the number of frames discarded by the routing entity.
OutUnicastFrames	Shows the number of outgoing unicast frames routed.
OutMulticastFrames	Shows the number of outgoing multicast frames routed.

Viewing DHCP statistics for an interface

View DHCP statistics to manage network performance.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **IP**.
2. Click **DHCP Relay**.
3. Click the **Interfaces Stats** tab.

Interfaces Stats field descriptions

Use the data in the following table to use the **Interfaces Stats** tab.

Name	Description
IfIndex	Identifies the physical interface.
AgentAddr	Shows the IP address configured as the relay on this interface. This address is either the IP of the physical interface or the IP of the VRRP address.
NumRequests	Shows the number of DHCP and BootP requests on this interface.
NumReplies	Shows the number of DHCP and BootP replies on this interface.

Graphing DHCP statistics for a port

View DHCP statistics to manage network performance.

Procedure

1. In the Device Physical View, select a port.
2. In the navigation tree, expand the following folders: **Configuration** > **Graph**.
3. Click **Port**.
4. Click the **DHCP** tab.

5. Select one or more values.
6. Click the type of graph to create.

DHCP field descriptions

The following table describes parameters on the **DHCP** tab.

Name	Description
NumRequests	The number of DHCP and/or BootP requests on this interface.
NumReplies	The number of DHCP and/or BootP replies on this interface.

Viewing DHCP statistics for a port

View DHCP statistics to manage network performance.

Procedure

1. In the Device Physical view, select a port.
2. In the navigation tree, open the following folders: **Configuration** > **Edit** > **Port**
3. Click **IP**.
4. Click the **DHCP Relay** tab.
5. Click **Graph**.
6. Select one or more values.
7. Click the type of graph.

DHCP Stats field descriptions

Use the data in the following table to use the **DHCP Stats** tab.

Name	Description
NumRequests	The number of DHCP and BootP requests on this interface.
NumReplies	The number of DHCP and BootP replies on this interface.

Graphing DHCP statistics for a VLAN

View DHCP statistics to manage network performance.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**
2. Click **VLANs**.
3. On the **Basic** tab, select a VLAN.

4. Click **IP**.
5. Click the **DHCP Relay** tab.
6. Click **Graph**.
7. Select one or more values.
8. Click the type of graph.

DHCP Stats field descriptions

Use the data in the following table to use the **DHCP Stats** tab.

Name	Description
NumRequests	The number of DHCP and BootP requests on this interface.
NumReplies	The number of DHCP and BootP replies on this interface.

Displaying DHCP-relay statistics for Option 82

Display DHCP-relay statistics for all interfaces to manage network performance.

Procedure

1. In the Navigation tree, expand the following folders: **Configuration** > **IP**.
2. Click **DHCP-Relay**.
3. Click the **Option 82 Stats** tab.

Option 82 Stats field descriptions

Use the data in the following table to use the **Option 82 Stats** tab.

Name	Description
IfIndex	Shows the name of the interface on which you enabled option 82. Shows the port number if the interface is a brouter port or the VLAN number if the interface is a VLAN.
AgentAddr	Shows the IP address configured as the relay on this interface. This address is either the IP of the physical interface or the IP of the VRRP address.
FoundOp82	Shows the number of packets that the interface received that already had option82 in them.
Dropped	Shows the number of packets the interface dropped because of option 82–related issues. These reasons could be that the packet was received from an untrusted source or spoofing was detected. To

Table continues…

Name	Description
	determine the cause of the drop, you must enable trace on level 170.
CircuitId	Shows the value inserted in the packets as the circuit ID. The value is the index of the interface.
AddedCircuitId	Shows how many packets (requests from client to server) the circuit ID was inserted for that interface. If you expect this value to increase but it does not, and the interface does not drop a packet, it is possible the packet does not have enough space to insert the option. You must enable trace on level 170 to determine the cause.
RemovedCircuitId	Shows how many packets (replies from server to client) the circuit id was removed for that interface.
RemoteId	Shows the value inserted in the packets as the remote ID. The value is the MAC address of the interface.
AddedRemoteId	Shows how many packets (requests from client to server) the remote ID was inserted for that interface. If you expect this value to increase but it does not, and the interface does not drop a packet, it is possible the packet does not have enough space to insert the option. You must enable trace on level 170 to determine the cause.
RemovedRemoteId	Shows how many packets (replies from server to client) the remote ID was removed for that interface.

Viewing port OSPF statistics

View port OSPF statistics to manage network performance.

This tab does not appear for all hardware models.

Procedure

1. On the Device Physical View, select a port.
2. In the navigation pane, expand the following folders: **Configuration** > **Graph**.
3. Click **Port**.
4. Click the **OSPF** tab.

OSPF field descriptions

The following table describes parameters on the **OSPF** tab.

Name	Description
VersionMismatches	Specifies the number of version mismatches received by this interface.
AreaMismatches	Specifies the number of area mismatches received by this interface.
AuthTypeMismatches	Specifies the number of authentication type mismatches received by this interface.
AuthFailures	Specifies the number of authentication failures.
NetmaskMismatches	Specifies the number of net mask mismatches received by this interface.
HelloIntervalMismatches	Specifies the number of hello interval mismatches received by this interface.
DeadIntervalMismatches	Specifies the number of dead interval mismatches received by this interface.
OptionMismatches	Specifies the number of option mismatches in the hello interval or dead interval fields received by this interface.
RxHellos	Specifies the number of hello packets received by this interface.
RxDBDescrs	Specifies the number of database descriptor packets received by this interface.
RxLSUpdates	Specifies the number of link state update packets received by this interface.
RxLSReqs	Specifies the number of link state request packets received by this interface.
RxLSAcks	Specifies the number of link state acknowledge packets received by this interface.
TxHellos	Specifies the number of hello packets transmitted by this interface.
TxDBDescrs	Specifies the number of database descriptor packets transmitted by this interface.
TxLSUpdates	Specifies the number of link state update packets transmitted by this interface.
TxLSReqs	Specifies the number of link state request packets transmitted by this interface.
TxLSAcks	Specifies the number of link state acknowledge packets transmitted by this interface.

Viewing LACP port statistics

View LACP port statistics to monitor the performance of the port.

Procedure

1. In the Device Physical View, select a port.

2. In the navigation tree, expand the following folders: **Configuration** > **Graph**.
3. Click **Port**.
4. Click the **LACP** tab.
5. To change the poll interval, in the toolbar click the **Poll Interval** box, and then select a new interval.

LACP field descriptions

Use the data in the following table to view the LACP statistics.

Name	Description
LACPDUsRx	The number of valid LACPDU received on this aggregation port.
MarkerPDUsRx	The number of valid marker PDUs received on this aggregation port.
MarkerResponsePDUsRx	The number of valid marker response PDUs received on this aggregation port.
UnknownRx	The number of frames received that either: • carry Slow Protocols Ethernet type values, but contain an unknown PDU. • are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
IllegalRx	The number of frames received that carry the Slow Protocols Ethernet Type value (43B.4), but contain a badly formed PDU or an illegal value of Protocol Subtype (43B.4).
LACPDUsTx	The number of LACPDUs transmitted on this aggregation port.
MarkerPDUsTx	The number of marker PDUs transmitted on this aggregation port.
MarkerResponsePDUsTx	The number of marker response PDUs transmitted on this aggregation port.

Displaying available file storage

Display the amount of memory used and available for file storage.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **Storage Usage** tab.

Storage Usage field descriptions

Use the data in the following table to use the Storage Usage tab.

Name	Description
IntflashBytesUsed or **FlashBytesUsed**	Specifies the number of bytes used in internal flash memory.
IntflashBytesFree or **FlashBytesFree**	Specifies the number of bytes available for use in internal flash memory.
IntflashNumFiles or **FlashNumFiles**	Specifies the number of files in internal flash memory.
UsbBytesUsed	Specifies the number of bytes used in USB storage. This field does not appear for all hardware models.
UsbBytesFree	Specifies the number of bytes available for use in USB storage. This field does not appear for all hardware models.
UsbNumFiles	Specifies the number of files in USB storage. This field does not appear for all hardware models.

Viewing port policer statistics

View port policer statistics to manage network performance.

This tab does not appear for all hardware models.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Graph**.
2. Click **Port**.
3. Click the **Policer** tab.

Policer field descriptions

Use the data in the following table to use the Policer tab.

Name	Description
TotalPkts	Shows the total number of packets received on the port.
TotalBytes	Shows the total number of bytes received on the port.
YellowBytes	Shows the total number of bytes received on the port that were above the committed rate but below the peak rate.
RedBytes	Shows the total number of bytes received on the port that were above the peak rate.

Viewing ACE port statistics

About this task

Use port statistics to ensure that the ACE is operating correctly.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select a field on the **ACL** tab.
5. Click **ACE**.
6. Click the **Statistics** tab.

Statistics field descriptions

Use the data in the following table to use the **Statistics** tab.

Name	Description
AclId	Specifies the associated ACL index.
AceId	Specifies the ACE index.
MatchCountPkts	Specifies a packet count of the matching packets.
MatchCountOctets	Specifies the number of octets of the matching packets.

Viewing ACL statistics

About this task

Graph statistics for a specific ACL ID to view default statistics.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select an ACL.
5. Click **Graph**.
6. You can click **Clear Counters** to clear the **Statistics** fields.

Statistics field descriptions

Use the data in the following table to use the **Statistics** tab.

Name	Description
AclId	Specifies the ACL ID.
MatchDefaultSecurityPkts	Shows a security packet count of traffic that does not match an ACE rule or hits the default action if count is configured in the ACL global action.
MatchDefaultSecurityOctets	Shows a security byte count of traffic that does not match an ACE rule or hits the default action if count is configured in the ACL global action.
MatchDefaultQosPkts	Shows a QoS packet count of traffic that does not match an ACE rule or hits the default action if count is configured in the ACL global action.
MatchDefaultQosOctets	Shows a QoS byte count of traffic that does not match an ACE rule or hits the default action if count is configured in the ACL global action.
MatchGlobalSecurityPkts	Shows a security packet count of traffic that matches an ACE rule or hits the default action if count is configured in the ACL global action.
MatchGlobalSecurityOctets	Shows a security byte count of traffic that matches an ACE rule or hits the default action if count is configured in the ACL global action.
MatchGlobalQosPkts	Shows a QoS packet count of traffic that matches an ACE rule or hits the default action if count is configured in the ACL global action.
MatchGlobalQosOctets	Shows a QoS byte count of traffic that matches an ACE rule or hits the default action if count is configured in the ACL global action.

Clearing ACL statistics

About this task

Clear ACL statistics when you want to gather a new set of statistics.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select a field.
5. Click **ClearStats**.

Viewing VLAN and Spanning Tree CIST statistics

About this task

View CIST port statistics to manage network performance.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.
2. Click **MSTP**.
3. Click the **CIST Port** tab.
4. Select a port, and then click **Graph**.

CIST Port Stats field descriptions

The following table describes parameters on the CIST Port Stats tab.

Name	Descriptions
ForwardTransitions	Specifies the number of times this port has transitioned to the forwarding state.
RxMstBpduCount	Specifies the number of MSTP BPDUs received on this port.
RxRstBpduCount	Specifies the number of RSTP BPDUs received on this port.
RxConfigBpduCount	Specifies the number of configuration BPDUs received on this port.
RxTcnBpduCount	Specifies the number of TCN BPDUs received on this port.
TxMstBpduCount	Specifies the number of MSTP BPDUs transmitted from this port.
TxRstBpduCount	Specifies the number of RSTP BPDUs transmitted from this port.
TxConfigBpduCount	Specifies the number of configuration BPDUs transmitted from this port.
TxTcnBpduCount	Specifies the number of TCN BPDUs transmitted from this port.
InvalidMstBpduRxCount	Specifies the number of Invalid MSTP BPDUs received on this port.
InvalidRstBpduRxCount	Specifies the number of Invalid RSTP BPDUs received on this port.
InvalidConfigBpduRxCount	Specifies the number of invalid configuration BPDUs received on this port.
InvalidTcnBpduRxCount	Specifies the number of invalid TCN BPDUs received on this port. The number of times this port has migrated from one STP protocol version to another. The relevant protocols are STP-compatible and RSTP/MSTP. A trap is generated on the occurrence of this event.
ProtocolMigrationCount	Specifies the number of times this port has migrated from one STP protocol version to another. The relevant protocols are STP-compatible and RSTP. A trap is generated on the occurrence of this event.

Viewing VLAN and Spanning Tree MSTI statistics

About this task

View multiple spanning tree instance (MSTI) port statistics to manage network performance.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.
2. Click **MSTP**.
3. Click the **MSTI Port** tab.
4. Select a port, and then click **Graph**.

MSTI field descriptions

The following table describes parameters on the **MSTI** tab.

Name	Description
ForwardTransitions	Specifies the number of times this port has transitioned to the forwarding state for this specific instance.
ReceivedBPDUs	Specifies the number of BPDUs received by this port for this spanning tree instance.
TransmittedBPDUs	Specifies the number of BPDUs transmitted on this port for this spanning tree instance.
InvalidBPDUsRcvd	Specifies the number of invalid BPDUs received on this port for this spanning tree instance.

Viewing VRRP interface stats

About this task

View VRRP statistics to manage network performance.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **IP**.
2. Click **VRRP**.
3. Select the **Interface** tab.
4. Select an interface.
5. Click **Graph**.

Interface field descriptions

The following table describes parameters on the **Interface** tab.

Name	Description
AdvertiseRcvd	Specifies the number of VRRP advertisements received by this virtual router.
AdvertiseIntervalErrors	Specifies the number of received VRRP advertisement packets with a different interval is than configured for the local virtual router.
IPTtlErrors	Specifies the number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.
PriorityZeroPktsRcvd	Specifies the number of VRRP packets received by the virtual router with a priority of 0.
PriorityZeroPktsSent	Specifies the number of VRRP packets sent by the virtual router with a priority of 0'.
InvalidTypePktsRcvd	Specifies the number of VRRP packets received by the virtual router with an invalid value in the 'type' field.
AddressListErrors	Specifies the packets received address list the address list does not match the locally configured list for the virtual router.
AuthTypeMismatch	Specifies the count of authentication type mismatch messages.
PacketLengthErrors	Specifies the count of packet length errors.
AuthFailures	Specifies the count of authentication failure messages.

Viewing VRRP statistics

About this task

View VRRP statistics to monitor network performance.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **IP**.
2. Click **VRRP**.
3. Select the **Stats** tab.

Stats field descriptions

The following table describes parameters on the VRRP statistics tab.

Name	Description
ChecksumErrors	Specifies the number of VRRP packets received with an invalid VRRP checksum value.

Table continues…

Name	Description
VersionErrors	Specifies the number of VRRP packets received with an unknown or unsupported version number.
VrIDErrors	Specifies the number of VRRP packets received with an invalid VrID for this virtual router.

Viewing SMLT statistics

View SMLT statistics to manage network performance.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **VLAN**.
2. Click **MLT/LACP**.
3. Select the **Ist/SMLT Stats** tab.

IST/SMLT Stats field descriptions

The following table describes parameters on the IST/SMLT Stats tab.

Name	Description
SmltIstDownCnt	The number of times the session between the two peering switches has gone down since last boot.
SmltHelloTxMsgCnt	The count of transmitted hello messages.
SmltHelloRxMsgCnt	The count of received hello messages.
SmltLearnMacAddrTxMsgCnt	The count of transmitted learned MAC address messages.
SmltLearnMacAddrRxMsgCnt	The count of received learned MAC address messages.
SmltMacAddrAgeOutTxMsgCnt	The count of transmitted aging out MAC address messages.
SmltMacAddrAgeOutRxMsgCnt	The count of received aging out MAC address messages.
SmltMacAddrAgeExpTxMsgCnt	The count of transmitted MAC address age expired messages.
SmltMacAddrAgeExpRxMsgCnt	The count of received MAC address age expired messages.
SmltStgInfoTxMsgCnt	The count of transmitted STG information messages.
SmltStgInfoRxMsgCnt	The count of received STG information messages.
SmltDelMacAddrTxMsgCnt	The count of transmitted MAC address deleted messages.

Table continues…

Name	Description
SmltDelMacAddrRxMsgCnt	The count of received MAC address received messages.
SmltSmltDownTxMsgCnt	The count of transmitted SMLT down messages.
SmltSmltDownRxMsgCnt	The count of received SMLT down messages
SmltUpTxMsgCnt	The count of transmitted SMLT up messages.
SmltUpRxMsgCnt	The count of received SMLT up messages.
SmltSendMacTblTxMsgCnt	The count of sent send MAC table messages.
SmltSendMacTblRxMsgCnt	The count of received send MAC table messages.
SmltIgmpTxMsgCnt	The count of sent IGMP messages.
SmltIgmpRxMsgCnt	The count of received IGMP messages.
SmltPortDownTxMsgCnt	The count of sent port down messages.
SmltPortDownRxMsgCnt	The count of received port down messages.
SmltReqMacTblTxMsgCnt	The count or sent MAC table request messages.
SmltReqMacTblRxMsgCnt	The count of received MAC table request messages.
SmltRxUnknownMsgTypeCnt	The count of received unknown message type messages.
SmltPortTblSyncReqTxMsgCnt	The count of sent sync request messages.
SmltPortTblSyncReqRxMsgCnt	The count of received sync request messages.
SmltPortTblSyncTxMsgCnt	The count of sent sync messages.
SmltPortTblSyncRxMsgCnt	The count of received sync messages.
SmltPortUpdateTxMsgCnt	The count of sent update messages.
SmltPortUpdateRxMsgCnt	The count of received update messages.
SmltEntryUpdateTxMsgCnt	The count of sent entry update messages.
SmltEntryUpdateRxMsgCnt	The count of received entry update messages.
SmltDialectNegotiateTxMsgCnt	The count of sent protocol ID messages.
SmltDialectNegotiateRxMsgCnt	The count of received protocol ID messages.
SmltUpdateRespTxMsgCnt	The count of sent update response messages.
SmltUpdateRespRxMsgCnt	The count of received update response messages.
SmltTransQHighWaterMarkMsgCnt	The count of transaction queue high watermark messages.
SmltPollCountHighWaterMarkCnt	The count of poll count high watermark.

Viewing RSTP status statistics

About this task

You can view status statistics for Rapid Spanning Tree Protocol (RSTP).

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.
2. Click **RSTP**.
3. In the **RSTP Status** tab, select a port, and then click **Graph**.

RSTP Status field descriptions

The following table describes the **RSTP Status** fields.

Name	Description
RxRstBpduCount	Specifies the number of RSTP BPDUs this port received.
RxConfigBpduCount	Specifies the number of configuration BPDUs this port received.
RxTcnBpduCount	Specifies the number of TCN BPDUs this port received.
TxRstBpduCount	Specifies the number of RSTP BPDUs this port transmitted.
TxConfigBpduCount	Specifies the number of Config BPDUs this port transmitted.
TxTcnBpduCount	Specifies the number of TCN BPDUs this port transmitted.
InvalidRstBpduRxCount	Specifies the number of invalid RSTP BPDUs this port received. A trap is generated on the occurrence of this event.
InvalidConfigBpduRx Count	Specifies the number of invalid configuration BPDUs this port received. A trap is generated on the occurrence of this event.
InvalidTcnBpduRxCount	Specifies the number of invalid TCN BPDUs this port received. A trap is generated on the occurrence of this event.
ProtocolMigrationCount	Specifies the number of times this port migrated from one STP protocol version to another. The relevant protocols are STP-Compatible and RSTP. A trap is generated on the occurrence of this event.

Viewing MLT interface statistics

About this task

Use MLT interface statistics tab to view interface statistics for the selected MLT.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **MLT/LACP**.
3. Click the **MultiLink/LACP Trunks** tab.
4. Select an MLT.
5. Click **Graph**.
6. Click the **Interface** tab.

Interface field descriptions

Use the data in the following table to use the Interface tab.

Name	Description
InOctets	Specifies the total number of octets received on the MLT interface, including framing characters.
OutOctets	Specifies the total number of octets transmitted out of the MLT interface, including framing characters.
InUcastPkts	Specifies the number of packets delivered by this MLT to higher level protocols that were not addressed to a multicast or broadcast address at this sublayer.
OutUcastPkts	Specifies the number of packets that higher–level protocols requested be transmitted that were not addressed to a multicast address at this MLT. This total number includes discarded or unsent packets.
InMulticastPkt	Specifies the number of packets delivered to this MLT that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.
OutMulticast	Specifies the total number of packets that higher-level protocols requested be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or unsent. For a MAC layer protocol, this number includes both Group and Functional addresses.
InBroadcastPkt	Specifies the number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
OutBroadcast	Specifies the total number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.
InLsmPkts	Specifies the total number of Link State Messaging (LSM) packets delivered on this MLT.
OutLsmPkts	Specifies the total number of Link State Messaging (LSM) packets transmitted on this MLT.

Viewing MLT Ethernet error statistics

About this task

Use MLT Ethernet error statistics to view the error statistics.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **MLT/LACP**.
3. Click the **MultiLink/LACP Trunks** tab.
4. Select an MLT, and then click **Graph**.
5. Click the **Ethernet Errors** tab.

Ethernet Errors field descriptions

Use the data in the following table to use the **Ethernet Errors** tab.

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

Table continues…

Name	Description
SQETestError	Specifies the number of times that the SQE test error message is generated by the PLS sublayer for a particular MLT. The SQE test error message is defined in section 7.2.2.2.4 of ANSI/ IEEE 802.3-1985.
DeferredTransmiss	Specifies the frame count for which the first transmission attempt on a particular MLT is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollFrames	Specifies a count of successfully transmitted frames on a particular MLT for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts object, the ifOutMulticastPkts object, or the ifOutBroadcastPkts object, and is not counted by the corresponding instance of the MultipleCollisionFrames object.
MultipleCollFrames	Specifies the successfully transmitted frame count on a particular MLT for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts object, the ifOutMulticastPkts object, or the ifOutBroadcastPkts object, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	Specifies the number of times that a collision is detected on a particular MLT later than 512 bit-times into the transmission of a packet; 512 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.
ExcessiveCollis	Specifies the frame count for which transmission on a particular MLT fails due to excessive collisions.

Viewing RIP statistics

Use statistics to help you monitor Routing Information Protocol (RIP) performance. You can also use statistics in troubleshooting procedures.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **IP**.
2. Click **RIP**.
3. Click the **Status** tab.

Status field descriptions

Use the data in the following table to use the **Status** tab.

Name	Description
Address	The IP address of the router interface.
RcvBadPackets	The number of RIP response packets received by the RIP process that were subsequently discarded for any reason (examples: a version 0 packet or an unknown command type).
RcvBadRoutes	The number of routes, in valid RIP packets, that were ignored for any reason (examples: unknown address family or invalid metric).
SentUpdates	The number of triggered RIP updates actually sent on this interface. This field explicitly does not include full updates sent containing new information.

Viewing OSPF chassis statistics

Use statistics to help you monitor Open Shortest Path First (OSPF) performance. You can also graph statistics for all OSPF packets transmitted by the switch.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **IP**.
2. Click **OSPF**.
3. Click the **Stats** tab.
4. To create a graph for OSPF statistics, select a column, and then select a graph type.

Stats field descriptions

Use the data in the following table to use the **Stats** tab.

Name	Description
LsdbTblSize	Specifies the number of entries in the link state database table.
TxPackets	Specifies the number of packets transmitted by OSPF.
RxPackets	Specifies the number of packets received by OSPF.
TxDropPackets	Specifies the number of packets dropped before being transmitted by OSPF.
RxDropPackets	Specifies the number of packets dropped before they are received by OSPF.
RxBadPackets	Specifies the number of packets received by OSPF that are bad.
SpfRuns	Specifies the number of SPF calculations performed by OSPF.
BuffersAllocated	Specifies the number of buffers allocated for OSPF.
BuffersFreed	Specifies the number of buffers freed by OSPF.
BufferAllocFailures	Specifies the number of times that OSPF has failed to allocate buffers.
BufferFreeFailures	Specifies the number of times that OSPF has failed to free buffers.
Routes	Specifies the count of OSPF routes.
Adjacencies	Specifies the count of OSPF adjacencies.
Areas	Specifies the count of OSPF areas.

Graphing OSPF statistics for a VLAN

Use statistics to help you monitor OSPF performance on a VLAN. You can also graph statistics for all OSPF packets.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. Click the **Basic** tab.
4. Select a **VLAN**.
5. Click **IP**.
6. Click the **OSPF** tab.
7. Click **Graph**.
8. Select one or more values.
9. Click the type of graph.

OSPF field descriptions

Use the data in the following table to use the **OSPF** tab.

Name	Description
VersionMismatches	Indicates the number of version mismatches received by this interface.
AreaMismatches	Indicates the number of area mismatches received by this interface.
AuthTypeMismatches	Indicates the number of AuthType mismatches received by this interface.
AuthFailures	Indicates the number of authentication failures.
NetMaskMistmatches	Indicates the number of net mask mismatches received by this interface.
HelloIntervalMismatches	Indicates the number of hello interval mismatches received by this interface.
DeadIntervalMismatches	Indicates the number of dead interval mismatches received by this interface.
OptionMismatches	Indicates the number of options mismatches received by this interface.
RxHellos	Indicates the number of hello packets received by this interface.

Table continues…

Name	Description
RxDBDescrs	Indicates the number of database descriptor packets received by this interface.
RxLSUpdates	Indicate the number of Link state update packets received by this interface.
RxLsReqs	Indicates the number of Link state request packets received by this interface.
RxLSAcks	Indicates the number of Link state acknowledge packets received by this interface.
TxHellos	Indicates the number of hello packets transmitted by this interface.
TxDBDescrs	Indicates the number of database descriptor packets transmitted by this interface.
TxLSUpdates	Indicate the number of Link state update packets transmitted by this interface.
TxLSReqs	Indicates the number of Link state request packets transmitted by this interface.
TxLSAcks	Indicates the number of Link state acknowledge packets transmitted by this interface.

Graphing OSPF statistics for a port

Use statistics to help you monitor OSPF performance on a VLAN. You can also graph statistics for all OSPF packets.

The **Graph** button does not appear for all hardware platforms.

Procedure

1. On the Device Physical View, select a port.
2. In the navigation pane, expand the following folders: **Configuration** > **Edit** > **Port**.
3. Click **IP**.
4. Click the **OSPF** tab.
5. Click **Graph**.
6. Select one or more values.
7. Click the type of graph.

OSPF field descriptions

Use the data in the following table to use the **OSPF** tab.

Name	Description
VersionMismatches	Indicates the number of version mismatches received by this interface.
AreaMismatches	Indicates the number of area mismatches received by this interface.
AuthTypeMismatches	Indicates the number of AuthType mismatches received by this interface.
AuthFailures	Indicates the number of authentication failures.
NetMaskMistmatches	Indicates the number of net mask mismatches received by this interface.
HelloIntervalMismatches	Indicates the number of hello interval mismatches received by this interface.
DeadIntervalMismatches	Indicates the number of dead interval mismatches received by this interface.
OptionMismatches	Indicates the number of options mismatches received by this interface.
RxHellos	Indicates the number of hello packets received by this interface.
RxDBDescrs	Indicates the number of database descriptor packets received by this interface.
RxLSUpdates	Indicate the number of Link state update packets received by this interface.
RxLsReqs	Indicates the number of Link state request packets received by this interface.
RxLSAcks	Indicates the number of Link state acknowledge packets received by this interface.
TxHellos	Indicates the number of hello packets transmitted by this interface.
TxDBDescrs	Indicates the number of database descriptor packets transmitted by this interface.
TxLSUpdates	Indicate the number of Link state update packets transmitted by this interface.
TxLSReqs	Indicates the number of Link state request packets transmitted by this interface.
TxLSAcks	Indicates the number of Link state acknowledge packets transmitted by this interface.

Viewing BGP global stats

View BGP global stats.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **IP**.
2. Click **BGP**.
3. Click the **Global Stats** tab.

Global Stats field descriptions

Use the data in the following table to use the BGP Global Stats tab.

Name	Description
AbsoluteValue	Displays the counter value.
Cumulative	Displays the total value since you opened the Stats tab.
Average/sec	Displays the average value for each second.
Minimum/sec	Displays the minimum value for each second.
Maximum/sec	Displays the maximum value for each second.
LastVal/sec	Displays the last value for each second.
Starts	Displays the number of times the BGP connection started.
Stops	Displays the number of times the BGP connection stopped.
Opens	Displays the number of times BGP opens TCP.
Closes	Displays the number of times BGP closes TCP.
Fails	Displays the number of times TCP attempts failed.
Fatals	Displays the number of times TCP crashes due to fatal error.
ConnExps	Displays the number of times the TCP retry timer expired.
HoldExps	Displays the number of times the hold timer expired.
KeepExps	Displays the number of times the keepalive timer expired.
RxOpens	Displays the number of open instances BGP receives.
RxKeeps	Displays the number of keepalive instances BGP receives.
RxUpdates	Displays the number of update instances BGP receives.
RxNotifys	Displays the number of notification instances BGP receives.
TxOpens	Displays the number of open instances BGP transmitted.

Table continues…

Name	Description
TxKeeps	Displays the number of keepalive instances BGP transmitted.
TxUpdates	Displays the number of updates instances BGP transmits.
TxNotifys	Displays the number of notification instances BGP transmits.
BadEvents	Displays the number of invalid events FSM received.
SyncFails	Displays the number of times FDB sync failed.
TrEvent	Displays the trace event.
RxECodeHeader	Displays the total header errors received.
RxECodeOpen	Displays the total open errors received.
RxECodeUpdate	Displays the total update errors received.
RxECodeHoldtimer	Displays the total hold timer errors received.
RxECodeFSM	Displays the total FSM errors received.
RxECodeCease	Displays the total cease errors received.
RxHdrCodeNoSync	Displays the header not synchronized errors received.
RxHdrCodeInvalidMsgLen	Displays the header invalid message length errors received.
RxHdrCodeInvalidMsgType	Displays the header invalid message type errors received.
RxOpCodeBadVer	Displays the open errors received for Bad Version.
RxOpCodeBadAs	Displays the open errors received for le Bad AS Number.
RxOpCodeBadRtID	Displays the open errors received for Bad BGP Rtr ID.
RxOpCodeUnsuppOption	Displays the open errors received for Unsupported Option.
RxOpCodeAuthFail	Displays the open errors received for Auth Failures.
RxOpCodeBadHold	Displays the open errors received for Bad Hold Value.
RxUpdCodeMalformedAttrList	Displays the update errors received for Malformed Attr List.
RxUpdCodeWelKnownAttrUnrecog	Displays the update errors received for Welknown Attr Unrecog.
RxUpdCodeWelknownAttrMiss	Displays the update errors received for Welknown Attr Missing.
RxUpdCodeAttrFlagError	Displays the update errors received for Attr Flag Error.

Table continues…

Name	Description
RxUpdCodeAttrLenError	Displays the update errors received for Attr Len Error.
RxUpdCodeBadORIGINAttr	Displays the update errors received for Bad ORIGIN Attr.
RxUpdCodeASRoutingLoop	Displays the update errors received for AS Routing Loop.
RxUpdCodeBadNHAttr	Displays the update errors received for Bad NEXT-HOP Attr.
RxUpdCodeOptionalAttrError	Displays the update errors received for Optional Attr Error.
RxUpdCodeBadNetworkField	Displays the update errors received for Bad Network Field.
RxUpdCodeMalformedASPath	Displays the update errors received for Malformed AS Path.
TxECodeHeader	Displays the total Header errors transmitted.
TxECodeOpen	Displays the total Open errors transmitted.
TxECodeUpdate	Displays the total Update errors transmitted.
TxECodeHoldtimer	Displays the total Hold timer errors transmitted.
TxECodeFSM	Displays the total FSM errors transmitted.
TxECodeCease	Displays the total Cease errors transmitted.
TxHdrCodeNoSync	Displays the header Not Synchronized errors transmitted.
TxHdrCodeInvalidMsgLen	Displays the header Invalid msg len errors transmitted.
TxHdrCodeInvalidMsgType	Displays the header Invalid msg type errors transmitted.
TxOpCodeBadVer	Displays the open errors transmitted for Bad Version.
TxOpCodeBadAs	Displays the open errors transmitted for Bad AS Number.
TxOpCodeBadRtID	Displays the open errors transmitted for Bad BGP Rtr ID.
TxOpCodeUnsuppOption	Displays the open errors transmitted for Unsupported Option.
TxOpCodeAuthFail	Displays the open errors transmitted for Auth Failures.
TxOpCodeBadHold	Displays the open errors transmitted for Bad Hold Value.
TxUpdCodeMalformedAttrList	Displays the update errors transmitted for Malformed Attr List.

Table continues…

Name	Description
TxUpdCodeWelknownAttrUnrecog	Displays the update errors transmitted for Welknown Attr Unrecog.
TxUpdCodeWelknownAttrMiss	Displays the update errors transmitted for Welknown Attr Missing.
TxUpdCodeAttrFlagError	Displays the update errors transmitted for Attr Flag Error.
TxUpdCodeAttrLenError	Displays the update errors transmitted for Attr Len Error.
TxUpdCodeBadORIGINAttr	Displays the update errors transmitted for Bad ORIGIN Attr.
TxUpdCodeASRoutingLoop	Displays the update errors transmitted for AS Routing Loop
TxUpdCodeBadNHAttr	Displays the update errors transmitted for Bad NEXT-HOP Attr
TxUpdCodeOptionalAttrError	Displays the update errors transmitted for Optional Attr Error.
TxUpdCodeBadNetworkField	Displays the update errors transmitted for Bad Network Field.
TxUpdCodeMalformedASPath	Displays the update errors transmitted for Malformed AS Path.

Viewing statistics for a VRF

About this task

View VRF statistics to ensure the instance is performing as expected.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **IP**.
2. Click **VRF**.
3. Select a VRF.
4. Click the **Stats** button.

Stats field descriptions

Use the data in the following table to use the **Stats** tab.

Name	Description
StatRouteEntries	Specifies the number of routes for this VRF.
StatFIBEntries	Specifies the number of Forwarding Information Base (FIB) entries for this VRF.

Showing RADIUS server statistics

About this task

Use the server statistics feature to display the number of input and output packets and the number of input and output bytes. Statistics from console ports are available to assist with debugging.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **RADIUS**.
3. Click the **RADIUS Servers Stats** tab.

RADIUS Server Stats field descriptions

Use the data in the following table to use the **RADIUS Server Stats** tab.

Name	Description
AddressType	Specifies the type of IP address. RADIUS supports IPv4 addresses only.
Address	Shows the IP address of the RADIUS server.
Used by	Identifies the client.
AccessRequests	Shows the number of access-response packets sent to the server; does not include retransmissions.
AccessAccepts	Shows the number of access-accept packets, valid or invalid, received from the server.
AccessRejects	Shows the number of access-reject packets, valid or invalid, received from the server.
BadResponses	Shows the number of invalid access-response packets received from the server.
PendingRequests	Shows the access-request packets sent to the server that have not yet received a response or that have timed out.
ClientRetries	Shows the number of authentication retransmissions to the server.
AcctOnRequests	Shows the number of accounting on requests sent to the server.
AcctOffRequests	Shows the number of accounting off requests sent to the server.
AcctStartRequests	Shows the number of accounting start requests sent to the server.
AcctStopRequests	Shows the number of accounting stop requests sent to the server.
AcctInterimRequests	Number of Accounting Interim requests sent to the server. **Important:** The AcctInterimRequests counter increments only if you select AcctIncludeCli from the RADIUS Global tab.

Table continues…

Name	Description
AcctBadResponses	Shows the number of Invalid responses discarded from the server.
AcctPendingRequests	Shows the number of requests waiting to be sent to the server.
AcctClientRetries	Shows the number of retries made to this server.
RoundTripTime	Shows the time difference between the instance when a RADIUS request is sent and the corresponding response is received.
AccessChallenges	Shows the number of RADIUS access-challenges packets sent to this server. This does not include retransmission.
NasIpAddress	Shows the RADIUS client NAS Identifier for this server.

Showing SNMP statistics

About this task

Display SNMP statistics to monitor the number of specific error messages, such as the number of messages that were delivered to SNMP but were not allowed.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **SNMP** tab.

SNMP field descriptions

Use the data in the following table to display SNMP statistics.

Name	Description
OutTooBigs	Shows the number of SNMP PDUs that the SNMP protocol entity generated and for which the value of the error-status field is `tooBig`.
OutNoSuchNames	Shows the number of SNMP PDUs that the SNMP protocol entity generated and for which the value of the error-status is `noSuchName`.
OutBadValues	Shows the number of SNMP PDUs that SNMP protocol entity generated and for which the value of the error-status field is `badValue`.
OutGenErrors	Shows the number of SNMP PDUs that the SNMP protocol entity generated and for which the value of the error-status field is `genErr`.
InBadVersions	Shows the number of SNMP messages that were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
InBadCommunityNames	Shows the number of SNMP messages delivered to the SNMP protocol entity that used an SNMP community name not known to the entity.

Table continues…

Name	Description
InBadCommunityUsers	Shows the number of SNMP messages delivered to the SNMP protocol entity that represented an SNMP operation not allowed by the SNMP community named in the message.
InASNParseErrs	Shows the number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP messages.
InTooBigs	Shows the number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is `tooBig`.
InNoSuchNames	Shows the number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is `noSuchName`.
InBadValues	Shows the number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is `badValue`.
InReadOnlys	Shows the number of valid SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is read-only. It is a protocol error to generate an SNMP PDU that contains the value `read-only` in the error-status field; this object is provided as a means of detecting incorrect implementations of the SNMP.
InGenErrors	Shows the number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is `genErr`.

Displaying IS-IS system statistics

Use the following procedure to display Intermediate-System-to-Intermediate-System (IS-IS) system statistics.

Procedure

1. In the navigation tree, choose **Configuration** > **IS-IS**.
2. Click **Stats**.
3. Click the **System Stats** tab.

System Stats field descriptions

Use the data in the following table to use the **System Stats** tab.

Name	Description
CorrLSPs	Indicates the number of corrupted in-memory link-state packets (LSPs) detected. LSPs received from the wire with a bad checksum are silently dropped and not counted.

Table continues…

Name	Description
AuthFails	Indicates the number of authentication key failures recognized by this Intermediate System.
LSPDbaseOloads	Indicates the number of times the LSP database has become overloaded.
ManAddrDropFromAreas	Indicates the number of times a manual address has been dropped from the area.
AttmptToExMaxSeqNums	Indicates the number of times the IS has attempted to exceed the maximum sequence number.
SeqNumSkips	Indicates the number of times a sequence number skip has occurred.
OwnLSPPurges	Indicates the number of times a zero-aged copy of the system's own LSP is received from some other node.
IDFieldLenMismatches	Indicates the number of times a PDU is received with a different value for ID field length to that of the receiving system.
PartChanges	Indicates partition changes.
AbsoluteValue	Displays the counter value.
Cumulative	Displays the total value since you opened the Stats tab.
Average/sec	Displays the average value for each second.
Minimum/sec	Displays the minimum value for each second.
Maximum/sec	Displays the maximum value for each second.
LastVal/sec	Displays the last value for each second.

Displaying IS-IS interface counters

Use the following procedure to display IS-IS interface counters.

Procedure

1. From the navigation tree, choose **Configuration** > **IS-IS**.
2. Click **Stats**.
3. Click the **Interface Counters** tab.

Interface Counters field descriptions

Use the data in the following table to use the Interface Counters tab.

Name	Description
Index	Shows a unique value identifying the IS-IS interface.
Type	Identifies the type of circuit that recorded the counter value.

Table continues…

Name	Description
AdjChanges	Shows the number of times an adjacency state change has occurred on this circuit.
InitFails	Shows the number of times initialization of this circuit has failed. This counts events such as PPP NCP failures. Failures to form an adjacency are counted by isisCircRejAdjs.
RejAdjs	Shows the number of times an adjacency has been rejected on this circuit.
IDFieldLenMismatches	Shows the number of times an IS-IS control PDU with an ID field length different to that for this system has been received.
MaxAreaAddrMismatches	Shows the number of times an IS-IS control PDU with a max area address field different to that for this system has been received.
AuthFails	Shows the number of times an IS-IS control PDU with the correct auth type has failed to pass authentication validation.
LANDesISChanges	Shows the number of times the Designated IS has changed on this circuit at this level. If the circuit is point to point, this count is zero.

Displaying IS-IS interface control packets

Use the following procedure to display IS-IS interface control packets.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **IS-IS**.
2. Click **Stats**.
3. Click the **Interface Control Packets** tab.

Interface Control Packets field descriptions

Use the data in the following table to use the **Interface Control Packets** tab.

Name	Description
Index	Shows a unique value identifying the Intermediate-System-to-Intermediate-System (IS-IS) interface.
Direction	Indicates whether the switch is sending or receiving the PDUs.
Hello	Indicates the number of IS-IS Hello frames seen in this direction at this level.
LSP	Indicates the number of IS-IS LSP frames seen in this direction at this level.
CSNP	Indicates the number of IS-IS Complete Sequence Number Packets (CSNP) frames seen in this direction at this level.

Table continues…

Name	Description
PSNP	Indicates the number of IS-IS Partial Sequence Number Packets (PSNP) frames seen in this direction at this level.

Graphing IS-IS interface counters

Use the following procedure to graph IS-IS interface counters.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **IS-IS**.
2. Click **IS-IS**.
3. Click the **Interfaces** tab.
4. Select an existing interface.
5. Click the **Graph** button.

Interface Counters field descriptions

The following table describes the fields in the **Interface Counters** tab.

Name	Description
InitFails	Indicates the number of times initialization of this circuit has failed. This counts events such as PPP NCP failures.
RejAdjs	Indicates the number of times an adjacency has been rejected on this circuit.
IDFieldLenMismatches	Indicates the number of times an Intermediate-System-to-Intermediate-System (IS-IS) control PDU with an ID field length different from that for this system has been received.
MaxAreaAddrMismatches	Indicates the number of times an IS-IS control PDU with a max area address field different from that for this system has been received.
AuthFails	Indicates the number of times an IS-IS control PDU with the correct auth type has failed to pass authentication validation.
LANDesISChanges	Indicates the number of times the Designated IS has changed on this circuit at this level. If the circuit is point to point, this count is zero.
AbsoluteValue	Displays the counter value.
Cumulative	Displays the total value since you opened the Stats tab.
Average/Sec	Displays the average value for each second.
Minimum/Sec	Displays the minimum value for each second.
Maximum/Sec	Displays the maximum value for each second.
Last Val/Sec	Displays the last value for each second.

Graphing IS-IS interface sending control packet statistics

Use the following procedure to graph IS-IS interface receiving control packet statistics.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **IS-IS**.
2. Click **IS-IS**.
3. Click the **Interfaces** tab.
4. Select an existing interface.
5. Click the **Graph** button.
6. Click the **Interface Sending Control Packets** tab.

Interface Sending Control Packets field descriptions

The following table describes the fields in the **Interface Sending Control Packets** tab.

Name	Description
Hello	Indicates the number of IS-IS Hello (IIH) PDUs seen in this direction at this level. Point-to-Point IIH PDUs are counted at the lowest enabled level: at L1 on L1 or L1L2 circuits, and at L2 otherwise.
LSP	Indicates the number of IS-IS LSP frames seen in this direction at this level.
CSNP	Indicates the number of IS-IS Complete Sequence Number Packet (CSNP) frames seen in this direction at this level.
PSNP	Indicates the number of IS-IS Partial Sequence Number Packets (PSNPs) seen in this direction at this level.
AbsoluteValue	Displays the counter value.
Cumulative	Displays the total value since you opened the Stats tab.
Average/Sec	Displays the average value for each second.
Minimum/Sec	Displays the minimum value for each second.
Maximum/Sec	Displays the maximum value for each second.
Last Val/Sec	Displays the last value for each second.

Graphing IS-IS interface receiving control packet statistics

Use the following procedure to graph IS-IS interface sending control packet statistics.

Procedure

1. From the navigation tree, choose **Configuration** > **IS-IS**.

2. Click **IS-IS**.
3. Click the **Interfaces** tab.
4. Select an existing interface.
5. Click the **Graph** button.
6. Click the **Interface Receiving Control Packets** tab.

Interface Receiving Control Packets field descriptions

The following table describes the fields in the **Interface Receiving Control Packets** tab.

Name	Description
Hello	Indicates the number of IS-IS Hello PDUs seen in this direction at this level. Point-to-Point IIH PDUs are counted at the lowest enabled level: at L1 on L1 or L1L2 circuits, and at L2 otherwise.
LSP	Indicates the number of IS-IS link-state packet (LSP) frames seen in this direction at this level.
CSNP	Indicates the number of IS-IS Complete Sequence Number Packet (CSNP) frames seen in this direction at this level.
PSNP	Indicates the number of IS-IS Partial Sequence Number Packets (PSNPs) seen in this direction at this level.
AbsoluteValue	Displays the counter value.
Cumulative	Displays the total value since you opened the Stats tab.
Average/Sec	Displays the average value for each second.
Minimum/Sec	Displays the minimum value for each second.
Maximum/Sec	Displays the maximum value for each second.
Last Val/Sec	Displays the last value for each second.

Graphing stat rate limit statistics for a port

View stat rate limit statistics to view the total dropped packets and bytes.

This tab does not appear for all hardware platforms.

Procedure

1. In the Device Physical View, select a port.
2. In the navigation pane, expand the following folders: **Configuration** > **Graph**.
3. Click **Port**.
4. Click the **Stat Rate Limit** tab.
5. Select one or more values.
6. Click the type of graph to create.

Stat rate limit field descriptions

Use the data in the following table to use the **Stat Rate Limit** tab.

Name	Description
DropPktRate	Indicates the drop packet rate.
DropByteRate	Indicates the drop byte rate.
DropTotalBytes	Indicates the total bytes dropped.
DropTotalPkts	Indicates the total packets dropped.

Viewing IPv6 statistics for an interface

View IPv6 statistics to view information about the IPv6 datagrams on an interface.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **IPv6**.
2. Click **IPv6**.
3. Click the **Interfaces** tab.
4. Select an interface.
5. Click **IfStats**.
6. **(Optional)** Select one or more values, and then click on the type of graph to graph the data.

Statistics field descriptions

Use the data in the following table to use the **Statistics** tab.

Name	Description
InReceives	Shows the total number of input datagrams received by the interface, including those received in error.
InHdrErrors	Shows the number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, and errors discovered in processing the IPv6 options.
InTooBigErrors	Shows the number of input datagrams that could not be forwarded because their size exceeded the link MTU of the outgoing interface.
InNoRoutes	Shows the number of input datagrams discarded because no route could be found to transmit them to their destination.

Table continues…

Name	Description
InAddrErrors	Shows the number of input datagrams discarded because the IPv6 address in the IPv6 header destination field was not a valid address to be received at this entity. This count includes invalid addresses, for example, ::0, and unsupported addresses, for example, addresses with unallocated prefixes. For entities which are not IPv6 routers and do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
InUnknownProtos	Shows the number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed, which is not always the input interface for some of the datagrams.
InTruncatedPkts	Shows the number of input datagrams discarded because the datagram frame did not carry enough data.
InDiscards	Shows the number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded, for example, for lack of buffer space. This counter does not include datagrams discarded while awaiting re-assembly.
InDelivers	Shows the total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which is not always the input interface for some of the datagrams.
OutForwDatagrams	Shows the number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter includes only those packets which were Source-Routed using this entity, and the Source-Route processing was successful. For a successfully forwarded datagram the counter of the outgoing interface is incremented.
OutRequests	Shows the total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. This counter does not include datagrams counted in **OutForwDatagrams**.
OutDiscards	Shows the number of output IPv6 datagrams for which no problem was encountered to prevent their

Table continues…

Name	Description
	transmission to their destination, but which were discarded, for example , for lack of buffer space. This counter includes datagrams counted in **OutForwDatagrams** if such packets met this (discretionary) discard criterion.
OutFragOKs	Shows the number of IPv6 datagrams that have been successfully fragmented at this output interface.
OutFragFails	Shows the number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.
OutFragCreates	Shows the number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
ReasmReqds	Shows the number of IPv6 fragments received which needed to be reassembled at this interface. This counter is incremented at the interface to which these fragments were addressed, which is not always the input interface for some of the fragments.
ReasmOKs	Shows the number of IPv6 datagrams successfully reassembled. This counter is incremented at the interface to which these datagrams were addressed, which is not always the input interface for some of the fragments.
ReasmFails	Shows the number of failures detected by the IPv6 re- assembly algorithm). This value is not necessarily a count of discarded IPv6 fragments because some algorithms can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed, which is not always the input interface for some of the fragments.
InMcastPkts	Shows the number of multicast packets received by the interface.
OutMcastPkts	Shows the number of multicast packets transmitted by the interface.

Viewing ICMP statistics

View ICMP statistics for ICMP configuration information.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **IPv6**.
2. Click **IPv6**.

3. Click **Interfaces** tab.
4. Select the interface on which you want to view the ICMP statistics.
5. Click **ICMPstats** option from the menu.

ICMP stats field descriptions

Use the data in the following table to use the ICMP **Statistics** tab.

Name	Description
InMsgs	Specifies the total number of ICMP messages which the entity received. **Note:** This counter includes all those counted by icmpInErrors.
InErrors	Specifies the number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
InDestUnreachs	Specifies the number of ICMP Destination Unreachable messages received by the interface.
InAdminProhibs	Specifies the number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
InTimeExcds	Specifies the number of ICMP Time Exceeded messages by the interface.
InParmProblems	Specifies the number of ICMP Parameter Problem messages received by the interface.
InPktTooBigs	Specifies the number of ICMP Packet Too Big messages received by the interface.
InEchos	Specifies the number of ICMP Echo (request) messages received by the interface.
InEchoReplies	Specifies the number of ICMP Echo Reply messages received by the interface.
InRouterSolicits	Specifies the number of ICMP Router Solicit messages received by the interface.
InRouterAdvertisements	Specifies the number of ICMP Router Advertisement messages received by the interface
InNeighborSolicits	Specifies the number of ICMP Neighbor Solicit messages received by the interface.
InNeighborAdvertisements	Specifies the number of ICMP Neighbor Advertisement messages received by the interface.

Table continues…

Name	Description
InRedirects	Specifies the number of ICMP Redirect messages received by the interface.
InGroupMembQueries	Specifies the number of ICMPv6 Group Membership Query messages received by the interface
InGroupMembResponses	Specifies the number of ICPv6 Group Membership Response messages received by the interface.
InGroupMembReductions	Specifies the number of ICMPv6 Group Membership Reduction messages received by the interface.
OutMsgs	Specifies the total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
OutErrors	Specifies the number of ICMP messages which this interface did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IPv6 to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
OutDestUnreachs	Specifies the number of ICMP Destination Unreachable messages sent by the interface.
OutAdminProhibs	Specifies the number of ICMP destination unreachable/communication administratively prohibited messages sent.
OutTimeExcds	Specifies the number of ICMP Time Exceeded messages sent by the interface.
OutParmProblems	Specifies the number of ICMP Parameter Problem messages sent by the interface.
OutPktTooBigs	Specifies the number of ICMP Packet Too Big messages sent by the interface.
OutEchos	Specifies the number of ICMP Echo (request) messages sent by the interface.
OutEchoReplies	Specifies the number of ICMP Echo Reply messages sent by the interface.
OutRouterSolicits	Specifies the number of ICMP Router Solicitation messages sent by the interface.
OutRouterAdvertisements	Specifies the number of ICMP Router Advertisement messages sent by the interface.
OutNeighborSolicits	Specifies the number of ICMP Neighbor Solicitation messages sent by the interface.
OutNeighborAdvertisements	Specifies the number of ICMP Neighbor Advertisement messages sent by the interface.

Table continues…

Name	Description
OutRedirects	Specifies the number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
OutGroupMembQueries	Specifies the number of ICMPv6 Group Membership Query messages sent.
OutGroupMembResponses	Specifies the number of ICMPv6 Group Membership Response messages sent.
OutGroupMembReductions	Specifies the number of ICMPv6 Group Membership Reduction messages sent.

Viewing IPv6 OSPF statistics

View OSPF statistics to analyze trends. You can also graph statistics for all OSPF packets transmitted by the switch.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **IPv6**.
2. Click **OSPF**.
3. Click **Stats**.

Stats field descriptions

Use the data in the following table to use the **Stats** tab.

Name	Description
TxPackets	Shows the count of sent packets.
RxPackets	Shows the count of received packets.
TxDropPackets	Shows the count of sent, dropped packets.
RxDropPackets	Shows the count of received, dropped packets.
RxBadPackets	Shows the count of received, bad packets.
SpfRuns	Shows the count of intra-area route table updates with calculations using this area link-state database.
LastSpfRun	Shows the count of the most recent SPF run.
LsdbTblSize	Shows the size of the link state database table.
BadLsReqs	Shows the count of bad link requests.
SeqMismatches	Shows the count of sequence mismatched packets.

Viewing IPv6 VRRP statistics

View IPv6 VRRP statistics to monitor network performance.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **IPv6**.
2. Click **VRRP**.
3. Click the **Stats** tab.

Stats field descriptions

Use the data in the following table to use the **Stats** tab.

Name	Description
ChecksumErrors	Shows the number of VRRP packets received with an invalid VRRP checksum value.
VersionErrors	Shows the number of VRRP packets received with an unknown or unsupported version number.
VrIdErrors	Shows the number of VRRP packets received with an invalid VrID for this virtual router.

Viewing IPv6 VRRP statistics for an interface

View IPv6 VRRP statistics for a VLAN or port.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **IPv6**.
2. Click **VRRP**.
3. Click the **Interface** tab.
4. Select an interface.
5. Click **Statistics**.

Statistics field descriptions

Use the data in the following table to use the **Statistics** tab.

Name	Description
MasterTransitions	Shows the total number of times that the state of this virtual router has transitioned to master. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at

Table continues…

Name	Description
	other times as indicated by the value of DiscontinuityTime.
RcdAdvertisements	Shows the total number of VRRP advertisements received by this virtual router. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
AdvIntervalErrors	Shows the total number of VRRP advertisement packets received for which the advertisement interval is different than the one configured for the local virtual router. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
IpTtlErrors	Shows the total number of VRRP packets received by the virtual router with IPv4 TTL (for VRRP over IPv4) or IPv6 Hop Limit (for VRRP over IPv6) not equal to 255. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
RcvdPriZeroPackets	Shows the total number of VRRP packets received by the virtual router with a priority of 0. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
SentPriZeroPackets	Shows the total number of VRRP packets sent by the virtual router with a priority of 0. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
RcvdInvalidTypePkts	Shows the number of VRRP packets received by the virtual router with an invalid value in the 'type' field. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
AddressListErrors	Shows the total number of packets received for which the address list does not match the locally configured list for the virtual router. Discontinuities in the value of this counter can occur at reinitialization of the management system, and at other times as indicated by the value of DiscontinuityTime.

Table continues…

Name	Description
PacketLengthErrors	Shows the total number of packets received with a packet length less than the length of the VRRP header. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
RcvdInvalidAuthentications	Shows the total number of packets received with an unknown authentication type.

Viewing IPv6 DHCP Relay statistics for a port

Display individual IPv6 DHCP Relay statistics for specific ports to manage network performance. You can also create a graph of selected statistical values.

Procedure

1. On the Device Physical view, select a port.
2. In the navigation pane, expand the following folders: **Configuration** > **IPv6**
3. Click the **DHCP Relay** tab.
4. Click the **Interface** tab.
5. Select the interface on which you want to view the IPv6 DHCP Relay statistics.
6. Click **Statistics**.
7. Select one or more values.
8. Click the type of graph.

Statistics field descriptions

Use the data in the following table to use the **Statistics** tab.

Name	Description
NumRequests	Shows the number of DHCP and BootP requests on this interface.
NumReplies	Shows the number of DHCP and BootP replies on this interface.

Displaying IPsec interface statistics

Use this procedure to view IPsec statistics and counter values for each IPsec-enabled interface.

About this task

If you select an interface on the **Stats** tab, you can click **Graph** to graph particular statistics for that interface.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **IPv6**.
2. Click **IPSec**.
3. Click the **Stats** tab.

Stats field descriptions

Use the data in the following table to use the **Stats** tab.

Name	Description
IfIndex	Shows the interface index for which the statistic is captured.
InSuccesses	Specifies the number of ingress packets IPsec successfully carries.
InSPViolations	Specifies the number of ingress packets IPsec discards since boot time because of a security policy violation.
InNotEnoughMemories	Specifies the number of ingress packets IPsec discards since boot time because not enough memory is available.
InAHESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the AH replay check fails.
InESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the ESP replay check fails.
InAHFailures	Specifies the number of ingress packets IPsec discards since boot time because the AH authentication check fails.
InESPFailures	Specifies the number of ingress packets IPsec discards since boot time because the ESP authentication check fails.
OutSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutSPViolations	Specifies the number of egress packets IPsec discards since boot time because a security policy violation occurs.
OutNotEnoughMemories	Specifies the number of egress packets IPsec discards since boot time because not enough memory is available since boot time.

Table continues…

Name	Description
generalError	Specifies a general error.
InAhSuccesses	Specifies the number of ingress packets IPsec carries because the AH authentication succeeds.
OutAHSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
InESPSuccesses	Specifies the number of ingress packets IPsec carries since boot time because the ESP authentication succeeds.
OutESPSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutKBytes	Specifies the total number of kilobytes on egress.
OutBytes	Specifies the total number of bytes on egress.
InKBytes	Specifies the total number of bytes on ingress.
InBytes	Specifies the total number of bytes on ingress.
TotalPacketsProcessed	Specifies the total number of packets processed.
TotalPacketsByPassed	Specifies the total number of packets bypassed.
OutAHFailures	Specifies the number of egress packets IPsec discards since boot time because the AH authentication check fails.
OutESPFailures	Specifies the number of egress packets IPsec discards since boot time because the ESP authentication check fails.
InMD5Hmacs	Specifies the number of inbound HMAC MD5 occurrences since boot time.
InSHA1Hmacs	Specifies the number of inbound HMAC SHA1 occurrences since boot time.
InAESXCBCs	Specifies the number of inbound AES XCBC MAC occurrences since boot time.
InAnyNullAuth	Specifies the number of inbound null authentication occurrences since boot time.
In3DESCBCs	Specifies the number of inbound 3DES CBC occurrences since boot time.
InAESCBCs	Specifies the number of inbound AES CBC occurrences since boot time.
InAESCTRs	Specifies the number of inbound AES CTR occurrences since boot time.
InAnyNulEncrypt	Specifies the number of inbound null occurrences since boot time. Used for debugging purposes.
OutMD5Hmacs	Specifies the number of outbound HMAC MD5 occurrences since boot time.

Table continues…

Name	Description
OutSHA1Hmacs	Specifies the number of outbound HMAC SHA1 occurrences since boot time.
OutAESXCBCs	Specifies the number of outbound AES XCBC MAC occurrences since boot time.
OutInAnyNullAuth	Specifies the number of outbound null authentication occurrences since boot time.
Out3DESCBCs	Specifies the number of outbound 3DES CBC occurrences since boot time.
OutAESCBCs	Specifies the number of outbound AES CBC occurrences since boot time.
OutAESCTRs	Specifies the number of outbound AES CTR occurrences since boot time.
OutInAnyNullEncrypt	Specifies the number of outbound null occurrences since boot time. Used for debugging purposes.

Displaying switch level statistics for IPsec-enabled interfaces

Use this procedure to view IPsec statistics and counter values at the switch level for all IPsec-enabled interfaces.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **IPv6**.
2. Click **IPSec**.
3. Click the **Global Stats** tab.

Global Stats field descriptions

Use the data in the following table to use the **Global Stats** tab.

Name	Description
InSuccesses	Specifies the number of ingress packets IPsec successfully carries.
InSPViolations	Specifies the number of ingress packets IPsec discards since boot time because of a security policy violation.
InNotEnoughMemories	Specifies the number of ingress packets IPsec discards since boot time because not enough memory is available.
InAHESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the AH replay check fails.

Table continues…

Name	Description
InESPReplays	Specifies the number of ingress packets IPsec discards since boot time because the ESP replay check fails.
InAHFailures	Specifies the number of ingress packets IPsec discards since boot time because the AH authentication check fails.
InESPFailures	Specifies the number of ingress packets IPsec discards since boot time because the ESP authentication check fails.
OutSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutSPViolations	Specifies the number of egress packets IPsec discards since boot time because a security policy violation occurs.
OutNotEnoughMemories	Specifies the number of egress packets IPsec discards since boot time because not enough memory is available since boot time.
generalError	Specifies a general error.
InAhSuccesses	Specifies the number of ingress packets IPsec carries because the AH authentication succeeds.
OutAHSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
InESPSuccesses	Specifies the number of ingress packets IPsec carries since boot time because the ESP authentication succeeds.
OutESPSuccesses	Specifies the number of egress packets IPsec successfully carries since boot time.
OutKBytes	Specifies the total number of kilobytes on egress.
OutBytes	Specifies the total number of bytes on egress.
InKBytes	Specifies the total number of bytes on ingress.
InBytes	Specifies the total number of bytes on ingress.
TotalPacketsProcessed	Specifies the total number of packets processed.
TotalPacketsByPassed	Specifies the total number of packets bypassed.
OutAHFailures	Specifies the number of egress packets IPsec discards since boot time because the AH authentication check fails.
OutESPFailures	Specifies the number of egress packets IPsec discards since boot time because the ESP authentication check fails.
InMD5Hmacs	Specifies the number of inbound HMAC MD5 occurrences since boot time.

Table continues…

Name	Description
InSHA1Hmacs	Specifies the number of inbound HMAC SHA1 occurrences since boot time.
InAESXCBCs	Specifies the number of inbound AES XCBC MAC occurrences since boot time.
InAnyNullAuth	Specifies the number of inbound null authentication occurrences since boot time.
In3DESCBCs	Specifies the number of inbound 3DES CBC occurrences since boot time.
InAESCBCs	Specifies the number of inbound AES CBC occurrences since boot time.
InAESCTRs	Specifies the number of inbound AES CTR occurrences since boot time.
InAnyNulEncrypt	Specifies the number of inbound null occurrences since boot time. Used for debugging purposes.
OutMD5Hmacs	Specifies the number of outbound HMAC MD5 occurrences since boot time.
OutSHA1Hmacs	Specifies the number of outbound HMAC SHA1 occurrences since boot time.
OutAESXCBCs	Specifies the number of outbound AES XCBC MAC occurrences since boot time.
OutInAnyNullAuth	Specifies the number of outbound null authentication occurrences since boot time.
Out3DESCBCs	Specifies the number of outbound 3DES CBC occurrences since boot time.
OutAESCBCs	Specifies the number of outbound AES CBC occurrences since boot time.
OutAESCTRs	Specifies the number of outbound AES CTR occurrences since boot time.
OutInAnyNullEncrypt	Specifies the number of outbound null occurrences since boot time. Used for debugging purposes.

Viewing EAPoL Authenticator statistics

Use EAPoL Authenticator statistics to display the Authenticator Port Access Entity (PAE) statistics for each selected port.

Procedure

1. On the Device Physical View, select the port you want to graph.

   A yellow outline appears around the selected ports

If you want to select multiple ports, press Ctrl and hold down the key while you click the ports you want to configure. A yellow outline appears around the selected ports.

2. In the navigation pane, expand the following folders: **Configuration** > **Graph**, and then click **Port**.
3. Click **EAPOL Stats**.
4. If you selected multiple ports, from the Graph port EAPoL Stats tab Show list, select: Absolute Value, Cumulative, Average/sec, Minimum/sec, Maximum/sec, or LastVal/sec.

EAPOL Stats field descriptions

The following table describes values on the **EAPOL Stats** tab.

Name	Description
InvalidFramesRx	Displays the number of EAPoL frames received by this Authenticator in which the frame type is not recognized.
EapLengthErrorFramesRx	Displays the number of EAPoL frames received by this Authenticator in which the Packet Body Length field is invalid.
StartFramesRx	Displays the number of EAPoL start frames received by this Authenticator.
EapFramesRx	Displays the number of EAPoL-EAP frames received by this Authenticator.
LogoffFramesRx	Displays the number of EAPoL Logoff frames received by this Authenticator.
LastRxFrameVersion	Displays the last received version of the EAPoL frame by this Authenticator.
LastRxFrameSource	Displays the source MAC address of the last received EAPoL frame by this Authenticator.
AuthEapFramesTx	Displays the number of EAPoL-EAP frames transmitted by the Authenticator.

Viewing Multihost status information

Use the following procedure to display multiple host status for a port.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** --> **Security** --> **Data Path**.
2. Click **802.1x–EAPOL**.
3. Click the **MultiHost Status** tab.

MultiHost status field descriptions

The following table describes values on the **MultiHost Status** tab.

Name	Description
PortNumber	Indicates the port number associated with this port.
ClientMACAddr	Indicates the MAC address of the client.
PaeState	Indicates the current state of the authenticator PAE state machine.
VlanId	Indicates the VLAN assigned to the client.

Viewing EAPoL session statistics

Use the following procedure to display multiple host session information for a port.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** --> **Security** --> **Data Path**.
2. Click **802.1x–EAPOL**.
3. Click the **MultiHost Session** tab.

MultiHost session field descriptions

The following table describes values on the **MultiHost Session** tab.

Name	Description
StatsPortNumber	Indicates the port number associated with this port.
StatsClientMACAddr	Indicates the MAC address of the client.
Id	Indicates the unique identifier for the session.
AuthenticMethod	Indicates the authentication method used to establish the session.
Time	Indicates the elapsed time of the session.
TerminateCause	Indicates the cause of the session termination.
UserName	Indicates the user name that represents the identity of the supplicant PAE.

Viewing non-EAPoL MAC information

Use this procedure to view non-EAPoL client MAC information on a port.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** --> **Security** --> **Data Path**.
2. Click **802.1x–EAPOL**.

3. Click the **NEAP Radius** tab.

NEAP Radius field descriptions

The following table describes values on the **NEAP Radius** tab.

Name	Description
MacPort	Indicates the port number associated with this port.
MacAddr	Indicates the MAC address of the client.
MacStatus	Indicates the authentication status of the non EAP host that is authenticated using the RADIUS server.
VlanId	Indicates the VLAN assigned to the client.

Viewing secure channel (SC) outbound statistics

Use this procedure to view the secure channel (SC) outbound statistics using EDM.

This feature is not supported on all hardware platforms. If you do not see this command in EDM, the feature is not supported on your hardware. For more information about feature support, see *Release Notes*.

Procedure

1. In the Device Physical View tab, select the port for which you need to view the SC outbound statistics.
2. In the navigation tree, expand the following folders: **Edit** > **Port** > **General**.
3. Click the **SC Outbound Stats** tab.

Note:

Use the **Clear Stats** button to the clear single-port secure channel outbound statistics. The **Clear Stats** button is not available to clear multiple-port secure channel outbound statistics.

SC Outbound Stats field descriptions

The following table describes the fields in the **SC Outbound Stats** tab.

Field	Description
ProtectedPkts	Specifies the number of integrity protected but not encrypted packets for this transmitting SC.
EncryptedPkts	Specifies the number of integrity protected and encrypted packets for this transmitting SC.

Table continues…

Field	Description
OctetsProtected	Specifies the number of plain text octets that are integrity protected but not encrypted on the transmitting SC.
OctetsEncrypted	Specifies the number of plain text octets that are integrity protected and encrypted on the transmitting SC.

Viewing secure channel (SC) inbound statistics

Use this procedure to view the secure channel (SC) inbound statistics using EDM.

This feature is not supported on all hardware platforms. If you do not see this command in EDM, the feature is not supported on your hardware. For more information about feature support, see *Release Notes*.

Procedure

1. In the Device Physical View tab, select the port for which you need to view the SC inbound statistics.
2. In the navigation pane, expand the following folders: **Edit** > **Port** > **General**.
3. Click the **SC Inbound Stats** tab.

Note:

Use the **Clear Stats** button to the clear single-port secure channel inbound statistics. The **Clear Stats** button is not available to clear multiple-port secure channel inbound statistics.

SC Inbound Stats field descriptions

The following table describes the fields in the **SC Inbound Stats** tab.

Field	Description
UnusedSAPkts	Specifies the summary of received unencrypted packets on all SAs of this secure channel, with MACsec *not* in strict mode.
NoUsingSAPkts	Specifies the summary of received packets that were discarded along with either encrypted packets or packets that were received with MACsec operating in strict mode.
LatePkts	Specifies the number of packets received that have been discarded for this secure channel (SC) with Replay Protect enabled.

Table continues…

Field	Description
	Note: The current release does not support Replay Protect.
NotValidPkts	Specifies the summary of packets that were discarded in all SAs of the SC because they were not valid with one of the following conditions: • MACsec was operating in strict mode. • The packets received were encrypted but contained erroneous fields.
InvalidPkts	Specifies the summary of all packets received that were not valid for this SC, with MACsec operating in *check* mode.
DelayedPkts	Specifies the summary of packets for this SC, with the packet number (PN) of the packets lower than the lower bound replay protection PN. **Note:** The current release does not support Replay Protect.
UncheckedPkts	The total number of packets for this SC that: • Were encrypted and had failed the integrity check. • Were *not* encrypted and had failed the integrity check. • Were received when MACsec validation was not enabled.
OKPkts	Specifies the total number of valid packets for all SAs of this secure channel.
OctetsValidated	Specifies the number of octets of plaintext recovered from received packets that were integrity protected but not encrypted.
OctetsDecrypted	Specifies the number of octets of plaintext recovered from received packets that were integrity protected and encrypted.

Viewing MACsec interface statistics

Use this procedure to view the MACsec interface statistics using EDM.

This feature is not supported on all hardware platforms. If you do not see this command in EDM, the feature is not supported on your hardware. For more information about feature support, see *Release Notes*.

Procedure

1. In the Device Physical View tab, select the port for which you need to view the MACsec interface statistics.
2. In the navigation tree, expand the following folders: **Edit** > **Port** > **General**.
3. Click the **MacSec Interface Stats** tab.

Note:

Use the **Clear Stats** button to the clear MACsec interface statistics. The **Clear Stats** button is available to clear single-port as well as multiple-port MACsec interface statistics.

MacSec interface field descriptions

The following table describes the fields in the **MacSec Interface Stats** tab.

Field	Description
TxUntaggedPkts	Specifies the number of transmitted packets without the MAC security tag (SecTAG), with MACsec disabled on the interface.
TxTooLongPkts	Specifies the number of transmitted packets discarded because the packet length is greater than the maximum transmission unit (MTU) of the common port interface.
RxUntaggedPkts	Specifies the number of received packets without the MAC security tag (SecTAG), with MACsec *not* operating in strict mode.
RxNoTagPkts	Specifies the number of received packets without the MAC security tag (SecTAG), with MACsec operating in strict mode.
RxBadTagPkts	Specifies the number of received packets discarded with an invalid SecTAG, or with a zero value packet number (PN), or invalid Integrity Check Value (ICV).
RxUnknownSCIPkts	Specifies the number of packets received with an unknown secure channel identifier (SCI), and with MACsec *not* operating in strict mode.
RxNoSCIPkts	Specifies the number of packets received with an unknown secure channel identifier (SCI), and with MACsec operating in strict mode.
RxOverrunPkts	Specifies the number of packets discarded because the number of received packets exceeded the cryptographic performance capabilities.

Glossary

American Standard Code for Information Interchange (ASCII)	A code to represent characters in computers. ASCII uses uppercase and lowercase alphabetic letters, numeric digits, and special symbols.
Autonomous System (AS)	A set of routers under a single technical administration, using a single IGP and common metrics to route packets within the Autonomous System, and using an EGP to route packets to other Autonomous Systems.
Autonomous System Number (ASN)	A two-byte number that is used to identify a specific AS.
bit error rate (BER)	The ratio of the number of bit errors to the total number of bits transmitted in a specific time interval.
Bootstrap Protocol (BootP)	A User Datagram Protocol (UDP)/Internet Protocol (IP)-based protocol that a booting host uses to configure itself dynamically and without user supervision.
Collecting process	A process that receives flow records from one or more exporting processes. The collecting process can process or store received flow records.
Collector	A device that hosts one or more collecting processes.
cyclic redundancy check (CRC)	Ensures frame integrity is maintained during transmission. The CRC performs a computation on frame contents before transmission and on the receiving device. The system discards frames that do not pass the CRC.
Data flowset	One or more records, of the same type, in an export packet. Each record is either a flow data record or an options data record previously defined by a template record or an options template record.
Dynamic Random Access Memory (DRAM)	A read-write random-access memory, in which the digital information is represented by charges stored on the capacitors and must be repeatedly replenished to retain the information.
Exporting process	An export process that sends flow records to one or more collecting processes. One or more metering processes generate the flow records.

External Data Representation (XDR)	An IETF standard, RFC 1832, for the description and encoding of data.
Flow key	A field used to define a flow is termed a flow key. A flow key is each field that belongs to the packet header (for example, destination IP address), is a property of the packet itself (for example, packet length), or is derived from packet treatment (for example, AS number).
Flow record	A flow record contains information about a specific flow that was observed at an observation point. The flow record contains measured properties of the flow, for example, the total number of bytes for all packets in the flow, and characteristic properties of the flow, for example, source IP address.
Flowset	A generic term for a collection of flow records that use a similar structure. In an export packet, one or more flowsets follow the packet header. Three flow sets are available: template flowset, options template flowset, and data flowset.
forwarding database (FDB)	A database that maps a port for every MAC address. If a packet is sent to a specific MAC address, the switch refers to the forwarding database for the corresponding port number and sends the data packet through that port.
Frame Check Sequence (FCS)	Frames are used to send upper-layer data and ultimately the user application data from a source to a destination.
graphical user interface (GUI)	A graphical (rather than textual) computer interface.
Intermediate System to Intermediate System (IS-IS)	Intermediate System to Intermediate System(IS-IS) is a link-state, interior gateway protocol. ISO terminology refers to routers as Intermediate Systems (IS), hence the name Intermediate System to Intermediate System (IS-IS). IS-IS operation is similar to Open Shortest Path First (OSPF). In Shortest Path Bridging MAC (SPBM) networks, IS-IS discovers network topology and builds shortest path trees between network nodes that IS-IS uses for forwarding unicast traffic and determining the forwarding table for multicast traffic. SPBM employs IS-IS as the interior gateway protocol and implements additional Type-Length-Values (TLVs) to support additional functionality.
Internet Control Message Protocol (ICMP)	A collection of error conditions and control messages exchanged by IP modules in both hosts and gateways.
Internet Group Management Protocol (IGMP)	IGMP is a host membership protocol used to arbitrate membership in multicast services. IP multicast routers use IGMP to learn the existence of host group members on their directly attached subnets.

interswitch trunking (IST)	A feature that uses one or more parallel point-to-point links to connect two aggregation switches. The two aggregation switches use this channel to share information and operate as a single logical switch. Only one interswitch trunk can exist on each Split Multilink Trunking (SMLT) aggregation switch.
Layer 2	Layer 2 is the Data Link Layer of the OSI model. Examples of Layer 2 protocols are Ethernet and Frame Relay.
Layer 3	Layer 3 is the Network Layer of the OSI model. An example of a Layer 3 protocol is Internet Protocol (IP).
Link Aggregation Control Protocol Data Units (LACPDU)	Link aggregation control protocol data unit (LACPDU) is used for exchanging information among LACP-enabled devices.
link-state advertisement (LSA)	Packets that contain state information about directly connected links (interfaces) and adjacencies. Each Open Shortest Path First (OSPF) router generates the packets.
link-state database (LSDB)	A database built by each OSPF router to store LSA information. The router uses the LSDB to calculate the shortest path to each destination in the autonomous system (AS), with itself at the root of each path.
Logical Link Control (LLC)	A protocol used in LANs to transmit protocol data units between two end stations. This LLC layer addresses and arbitrates data exchange between two endpoints.
management information base (MIB)	The MIB defines system operations and parameters used for the Simple Network Management Protocol (SNMP).
media	A substance that transmits data between ports; usually fiber optic cables or category 5 unshielded twisted pair (UTP) copper wires.
Metering process	A process that generates flow records. An input to the process is packets observed at an observation point and packet treatment at the observation point. The metering process consists of a set of functions that includes packet header capturing, time stamping, sampling, classifying, and maintaining flow records. The maintenance of flow records can include creating new records, updating existing records, computing flow statistics, deriving further flow properties, detecting flow expiration, passing flow records to the exporting process, and deleting flow records.
multiplexing	Carriage of multiple channels over a single transmission medium; a process where a dedicated circuit is shared by multiple users. Typically, data streams intersperse on a bit or byte basis (time division), or separate by different carrier frequencies (frequency division).

nanometer (nm)	One billionth of a meter (10^{-9} meter). A unit of measure commonly used to express the wavelengths of light.
NonVolatile Random Access Memory (NVRAM)	Random Access Memory that retains its contents after electrical power turns off.
Observation point	An observation point is a network location where you can observe IP packets. Examples include a port or a VLAN.
Options data record	The data record that contains values and scope information of the flow measurement parameters that correspond to an options template record.
Options template flowset	One or more options template records in an export packet.
Options template record	A record that defines the structure and interpretation of fields in an options data record, including defining the scope within which the options data record is relevant.
policing	Ensures that a traffic stream follows the domain service-provisioning policy or service-level agreement (SLA).
Port Access Entity (PAE)	Software that controls each port on the switch. The PAE, which resides on the device, supports authenticator functionality. The PAE works with the Extensible Authentication Protocol over LAN (EAPoL).
Protocol Data Units (PDUs)	A unit of data that is specified in a protocol of a specific layer and that consists of protocol-control information of the specific layer and possibly user data of that layer.
quality of service (QoS)	QoS features reserve resources in a congested network, allowing you to configure a higher priority for certain devices. For example, you can configure a higher priority for IP deskphones, which need a fixed bit rate and split the remaining bandwidth between data connections if calls in the network are more important than the file transfers.
Random Access Memory (RAM)	Memory into which you can write and read data. A solid state memory device used for transient memory stores. You can enter and retrieve information from storage position.
remote login (rlogin)	An application that provides a terminal interface between hosts (usually UNIX) that use the TCP/IP network protocol. Unlike Telnet, rlogin assumes the remote host is, or behaves like, a UNIX host.
remote monitoring (RMON)	A remote monitoring standard for Simple Network Management Protocol (SNMP)-based management information bases (MIB). The Internetwork Engineering Task Force (IETF) proposed the RMON standard to provide guidelines for remote monitoring of individual LAN segments.

Shortest Path Bridging MAC (SPBM)	Shortest Path Bridging MAC (SPBM) uses the Intermediate-System-to-Intermediate-System (IS-IS) link-state routing protocol to provide a loop-free Ethernet topology that creates a shortest-path topology from every node to every other node in the network based on node MAC addresses. SPBM uses the 802.1ah MAC-in-MAC frame format and encapsulates the source bridge identifier into the B-MAC header. SPBM eliminates the need for multiple overlay protocols in the core of the network by reducing the core to a single Ethernet-based link-state protocol, which can provide virtualization services, both layer 2 and layer 3, using a pure Ethernet technology base.
shortest path first (SPF)	A class of routing protocols that use Djikstra's algorithm to compute the shortest path through a network, according to specified metrics, for efficient transmission of packet data.
Small Form Factor Pluggable (SFP)	A hot-swappable input and output enhancement component that allows gigabit Ethernet ports to link with other gigabit Ethernet ports over various media types.
Small Form Factor Pluggable plus (SFP +)	SFP+ transceivers are similar to SFPs in physical appearance but SFP+ transceivers provide Ethernet at 10 gigabits per second (Gbps).
spanning tree	A simple, fully-connected active topology formed from the arbitrary physical topology of connected bridged Local Area Network components by relaying frames through selected bridge ports. The protocol parameters and states that are used and exchanged to facilitate the calculation of the active topology and to control the bridge relay function.
Spanning Tree Group (STG)	A collection of ports in one spanning-tree instance.
time-to-live (TTL)	The field in a packet used to determine the valid duration for the packet. The TTL determines the packet lifetime. The system discards a packet with a TTL of zero.
traffic profile	The temporal properties of a traffic stream, such as rate.
Trivial File Transfer Protocol (TFTP)	A protocol that governs transferring files between nodes without protection against packet loss.
trunk	A logical group of ports that behaves like a single large port.
User Datagram Protocol (UDP)	In TCP/IP, a packet-level protocol built directly on the Internet Protocol layer. TCP/IP host systems use UDP for application-to-application programs.

Virtual Router Redundancy Protocol (VRRP)	A protocol used in static routing configurations, typically at the edge of the network. This protocol operates on multiple routers on an IP subnet and elects a primary gateway router. When the primary router fails, a backup router is quickly available to take its place.