ExtremeSwitching

Configuring System Monitoring on Ethernet Routing Switch 3600 Series

Release 6.3
9035804 Rev AA
August 2019

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: www.extremenetworks.com/support/policies/software-licensing

Contents

Chapter 1: About this Document

This section discusses the purpose of this document, the conventions used, ways to provide feedback, additional help, and information regarding other Extreme Networks publications.

Purpose

This guide provides information about system logging, displaying system statistics, and configuring network monitoring on the Extreme Networks ERS 3600 Series switches.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that can be used throughout this document.

Table 1: Notice Icons

Icon	Alerts you to...
Important:	A situation that can cause serious inconvenience.
Note:	Important features or instructions.
Tip:	Helpful tips and notices for using the product.
Danger:	Situations that will result in severe bodily injury; up to and including death.
Warning:	Risk of severe personal injury or critical loss of data.
Caution:	Risk of personal injury, system damage, or loss of data.

Table 2: Text Conventions

Convention	Description
Angle brackets (< >)	Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. If the command syntax is `cfm maintenance-domain maintenance-level <0-7>` , you can enter `cfm maintenance-domain maintenance-level 4`.
Bold text	Bold text indicates the GUI object name you must act upon. Examples: • Click **OK**. • On the **Tools** menu, choose **Options**.
Braces ({ })	Braces ({ }) indicate required elements in syntax descriptions. Do not type the braces when you enter the command. For example, if the command syntax is `ip address {A.B.C.D}`, you must enter the IP address in dotted, decimal notation.
Brackets ([ ])	Brackets ([ ]) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command. For example, if the command syntax is `show clock [detail]`, you can enter either `show clock` or `show clock detail`.
Ellipses (…)	An ellipsis (…) indicates that you repeat the last element of the command as needed. For example, if the command syntax is `ethernet/2/1 [ <parameter> <value> ]...`, you enter `ethernet/2/1` and as many parameter-value pairs as you need.
Italic Text	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.
`Plain Courier Text`	Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages.

Table continues…

Convention	Description
	Examples: • `show ip route` • `Error: Invalid command syntax [Failed][2013-03-22 13:37:03.303 -04:00]`
Separator (>)	A greater than sign (>) shows separation in menu paths. For example, in the Navigation tree, expand the **Configuration** > **Edit** folders.
Vertical Line (|)	A vertical line (|) separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command. For example, if the command syntax is `access-policy by-mac action { allow | deny }`, you enter either `access-policy by-mac action allow` or `access-policy by-mac action deny`, but not both.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
The Hub	A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
Call GTAC	For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form with your information (all fields are required).
3. Select the products for which you would like to receive notifications.

   Note:
   You can modify your product selections or unsubscribe at any time.
4. Click **Submit**.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Chapter 2: New in this document

There are no new feature changes in this release.

Chapter 3: System Monitoring

Use the information in this chapter to help you understand system monitoring and how to configure and use system monitoring features using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

System Monitoring fundamentals

This section contains information about the fundamental principles of System Monitoring.

CPU and memory utilization

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

The memory utilization provides information about the percentage of the dynamic memory currently used by the system. The switch displays memory utilization in terms of the lowest percentage of dynamic memory available since system startup.

No configuration is required for this display-only feature.

Light Emitting Diode display

The switch displays diagnostic and operation information though the LEDs on the unit. Familiarize yourself with the interpretation of the LEDs on the switch.

For more information about the interpretation of the LEDs, see Ethernet Routing Switch 3600 Series Quick Install Guide .

EDM MIB Web page

You can use the EDM MIB Web page to view the response of an SNMP Get and Get-Next request for an Object Identifier (OID) or object name.

With the SNMP walk, you can retrieve a subtree of the Management Information Base (MIB) that has the object as root by using Get-Next requests.

The MIB Web page does not support the following features:

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

SNMP traps

Simple Network Management Protocol (SNMP) traps are configured as notification controls.

For more information about notification controls, see Configuring Security on Ethernet Routing Switch 3600 Series .

System Log

The System Log displays messages obtained from system Non Volatile Random Access Memory (NVRAM) or Dynamic Random Access Memory (DRAM). The System Log displays only the data for the switch through the Console or Comm port or Telnet.

System Log messages operate as follows:

- NVRAM messages are retrievable after a system reset.
- DRAM messages can be viewed while the system is operational.
- All NVRAM and DRAM messages are time stamped.
- When you restart your system after a reset, the DRAM messages are deleted.
- After a reset, all messages stored in NVRAM are copied to DRAM (DRAM messages are not copied to NVRAM). The messages copied to DRAM are time stamped to zero (0).

Dual Syslog Server Support

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

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

The servers can use either an IPv4 or IPv6 address.

Software exception log

This feature allows an administrator to see software exceptions generated in the ERS 3600 Series switch. The types of software exceptions include:

- Data Access exceptions
- Program exceptions
- Watchdog exceptions (appear as NMI exceptions)
- Instruction Access exceptions

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

You can display and clear the last software exceptions generated in the system using CLI. See Software exception log using CLI on page 24.

Note:

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

Remote logging

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

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

After the IP address is in the system, syslog messages can be sent to the remote syslog server. If a syslog message is generated prior to capturing the IP address of the server, the system stores up to 10 messages that are sent after the IP address of the remote server is on the system.

You can configure this feature by enabling remote logging, specifying the IP address of the remote syslog server, and specifying the severity level of the messages to be sent to the remote server.

Port mirroring

With the Port mirroring feature, also referred to as conversation steering, you can allocate a single switch port (monitor port) as a traffic monitor for another switch port (mirror port). All incoming and/or outgoing traffic on the mirrored port is copied to the monitor port. This feature is helpful in network troubleshooting.

You can specify port-based monitoring for ingress and/or egress to a specific port. You can also attach a probe device or equivalent, to the designated monitor port. When a port is operating as a monitor port, forwarding is not allowed on that port.

Port mirroring configuration rules

The following configuration rules apply to the various port mirroring modes:

Port mirroring ingress mode (Xrx or ->Port X)—In the Port mirroring ingress mode, packets received on mirror port X are copied to the monitor port.

Standalone—On a standalone switch there is no limitation for ingress port mirroring.

Stack—To enable ingress port mirroring in a stack environment, the mirror port and the monitor port can be on any unit in the stack.

Port mirroring egress mode (Xtx or Port X ->)—In the Port mirroring egress mode, packets transmitted on mirror port X are copied to the monitor port.

Standalone—On a standalone switch, there is no limitation for ingress port mirroring.

Stack—To enable egress port mirroring in a stack environment, the mirror port and the monitor port can be on any unit in the stack.

Port mirroring ingress and egress mode (Xrx or Xtx or <->Port X)—In the Port Mirroring ingress and egress mode, packets that are either transmitted or received on mirror port X are copied to the monitor port.

Standalone—On a standalone switch, there is no limitation for ingress port mirroring.

Stack—Concurrent ingress and egress port mirroring is not supported in stack configurations.

Many to One Port Mirroring

The Many to One Port Mirroring feature provides the ability of mirroring multiple ports to a single monitor port. You can use this feature to configure a single port to capture traffic from a set of selected ports. The captured traffic can be ingress or egress traffic.

Modes

The following are the four modes of Many to One Port Mirroring:

- ManyToOneRx: Monitors all traffic received on the mirrored ports.
- ManyToOneTx: Monitors all traffic transmitted by the mirrored ports.
- ManyToOneRxTx: Monitors all traffic received or transmitted by the mirror ports.

- XrxOrYtx: Monitors all traffic received by port X or transmitted by port Y.

Configurations

Many to One Port Mirroring is supported in the following configurations:

- Stand-alone mode
- Stacking mode

The following table provides the port specifications for Many to One Port Mirroring:

Mode	Monitor port	Mirror port
ManyToOneRx	14	20, 21, 5-8
ManyToOneTx	14	20, 21, 5-8
ManyToOneRxTX	14	20, 21, 5-8
XrxOrYtx	14	18 (port X), 19 (port Y)

Limitations

The following are the Many to One Port Mirroring limitations:

- Only ingress and egress port traffic mirroring is supported.
- Can configure up to four mirror ports.
- Mirror ports must continue to perform normal frame switching operation.
- Cannot configure an MLT group as a monitor port.

Stack monitor

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

The stack monitor sends a trap for the following events.

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

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

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

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

For more information on configuring the stack monitor, refer to Stack health and monitoring configuration on page 28.

Unit uptime display

You can display the uptime for each unit in a stack. Unit stack uptime collects the stack uptime for each unit in a stack and reports this information when requested. You can determine how long each unit is connected to the stack. You can use CLI commands to display the unit uptimes.

To use CLI to display the unit uptime, see Displaying unit stack uptime on page 32.

Chassis and port statistics

Chassis and port statistics allow you to view detailed information about any switch or port. The port statistics are divided by received and transmitted so that you can compare and evaluate throughput or other port parameters.

Show environmental

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

You can display the following parameters for each switch:

- AC power supply status
- fan status
- system temperature

Note:

AC power supply status information is only available in EDM.

The Show Environmental output depends on the hardware of each unit. For example you can have 0 to 4 fans on one unit, depending on its type. Because the switches have only one primary power supply unit, this is the only one displayed.

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

Measurement	State	Description
AC power	Normal	If AC or AC/RPSU power is present.
	Unknown	Other unknown state.

Table continues…

Measurement	State	Description
Fan	OK	If the fan is working properly.
	FAIL	If any fan malfunction exists.
	N/A	If the fan does not exist.
Temperature	OK	If the temperature is lower than 50 deg. C. The actual temperature is also displayed after the status.
	HIGH	If the temperature is higher than 50 deg. C. The actual temperature is also displayed after the status.

For more information, see Displaying environmental status using CLI on page 32 and the EDM procedures beginning with Displaying switch power supply information using EDM on page 39.

System Monitoring Configuration using CLI

Use the procedures in this section to configure System Monitoring, using the CLI.

Displaying CPU Utilization

Display CPU utilization for all units or a specific unit.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show cpu-utilization unit <1-8>
   ```

Variable definitions

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

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

Displaying Memory Utilization

Display memory utilization for all units or a specific unit.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show memory-utilization unit <1-8>
   ```

Variable definitions

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

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

System logs using CLI

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

Displaying The System Event Log

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show logging
   ```

Variable definitions

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

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

Configuring system logging

Configure the system settings for the system event log.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   [no] [default] logging [enable|disable] [level critical|serious|
   informational|none] [nv-level critical|serious|none] remote
   [address|enable|facility|level|secondery-address] volatile [latch|
   overwrite]
   ```

Variable definitions

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

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

Clearing Log Messages

Clear all log messages in DRAM.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Variable definitions

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

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

Configuring Remote System Logging

Manage the logging of system messages on a remote server.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

Variable	Value
address <*A.B.C.D* | *WORD*>	Specifies the primary remote system log server IP address. • A.B.C.D is the IPv4 address of the remote server • WORD is the remote host IPv6 address. The value is a character string with a maximum of 45 characters.
enable	Enables system message logging on the remote server. You must configure either the primary or secondary remote server IP address before you can enable remote logging.
facility <*daemon*| *local0* | *local1* | *local2* | *local3* | *local4* | *local5* | *local6* | *local7*>	Specifies remote logging facility.
level<*critical*|*informational*|*none*|*serious*>	Specifies the level of system messages to send to the remote system log server: • critical —only events classified as critical are sent to the remote system log server • serious —only events classified as serious are sent to the remote system log server

Table continues…

Variable	Value
	• informational —only events classified as informational are sent to the remote log server • none —no system log messages are sent to the remote system log server
secondary-address<*A.B.C.D*|<*WORD*>	Specifies the secondary remote system log server IP address: • A.B.C.D. is the IPv4 address of the remote server • WORD is the remote host IPv6 address. The value is a character string with a maximum of 45 characters

Displaying system logging information

Configures information for system logging.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Example

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

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

lldpXMedTopologyChangeDetected,                                    Subtype = 4 Class
= 4
```

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

Variable definitions

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

Variable	Value
config	Displays local and remote system logging configuration status
critical	Displays critical log messages
informational	Displays informational log messages
serious	Displays serious log messages
sort-reverse	Displays informational log messages in reverse chronological order (beginning with most recent)
unit<*1–8*>	Specifies log messages for a specific switch in a stack

Disabling remote system logging

Disable the logging of system messages on a remote server.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Restoring remote system logging

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Software exception log

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

Displaying last generated software exception log

Display the last generated software exception log for debugging purposes.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Note:

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

Example

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

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

Clearing last generated software exception log

Erase the last generated software exception log after viewing.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   clear system last—exception [unit <1-8>]
   ```

Port statistics using CLI

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

Displaying port statistics

Use this procedure to display port statistics on both received and transmitted traffic.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

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

Example

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

```
Switch#show port-statistics port 1
Received
```

```
    Packets:                0
    Multicasts:             0
    Broadcasts:             0
    Total Octets:           0
    FCS Errors:             0
    Undersized Packets:     0
    Oversized Packets:      0
    Filtered Packets:       0
    Frame Errors:           0
    Pause Frames:           0
Transmitted:
    Packets:                0
    Multicasts:             0
    Broadcasts:             0
    Total Octets:           0
    Collisions:             0
    Single Collisions:      0
    Multiple Collisions:    0
    Excessive Collisions:   0
    Deferred Packets:       0
    Late Collisions:        0
    Pause Frames:           0
Packets     64 bytes:       0
            65-127 bytes:   0
            128-255 bytes:  0
            256-511 bytes:  0
            512-1023 bytes: 0
            1024-1518 bytes: 0
            Jumbo:          0
    Dropped on No Resources: 0
Switch#
```

Variable definitions

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

Variable	Value
port<*portlist*>	Specifies the port numbers for which to display statistics. If you omit this parameter, all ports are shown.

Note:

For a description of the output fields for this command, see Ethernet Errors tab field descriptions on page 58.

Displaying stack port statistics

Use this procedure to display the stack port counters.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Example

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

```
Switch (config)#show port-statistics unit 1
                           UP                  DOWN
-------------------------- ------------------- ------------------
Received
    Packets:                1189                1784
    Multicasts:             0                   68
    Broadcasts:             0                   0
    Total Octets:           1744739             1980750
    FCS Errors:             0                   0
    Undersized Packets:     0                   0
    Oversized Packets:      354                 384
    Filtered Packets:       0                   0
    Frame Errors:           0                   0
    Pause Frames:           0                   0
Transmitted:
    Packets:                3140                3738
    Multicasts:             385                 385
    Broadcasts:             0                   0
    Total Octets:           1040948             2981198
    Collisions:             0                   0
    Single Collisions:      0                   0
    Multiple Collisions:    0                   0
    Excessive Collisions:   0                   0
    Deferred Packets:       0                   0
    Late Collisions:        0                   0
    Pause Frames:           0                   0
Packets     64 bytes:       0                   0
            65-127 bytes:   1941                2550
            128-255 bytes:  349                 415
            256-511 bytes:  490                 499
            512-1023 bytes: 859                 875
            1024-1518 bytes: 329                348
            Jumbo:          361                 835
    Dropped on No Resources: 0                  0
```

Clearing Statistical Information

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

Procedure

1. Enter VLAN Interface Configuration mode:

   ```
   enable
   configure terminal
   interface vlan <vlan ID>
   ```

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

   ```
   clear-stats [port <portlist>]
   ```

Variable definitions

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

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

Stack health and monitoring configuration

You can use Stack Health and Monitoring for more robust switch discovery and to obtain additional information about stack communication failure. This section describes how to view and configure stack health parameters.

Displaying stack health

Use this procedure to view the stack health information. The stack health information displays the rear port status for each unit and confirms the number of switching units in the stack.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show stack health
   ```

Example

The following figure provides a sample of the **`show stack health`** command.

```
Switch#show stack health

--------------------------------------------------------------------------------
UNIT#            Switch Model       Cascade Up            Cascade Down
--------------------------------------------------------------------------------
1 (Base)          3626GTS            OK                    OK
2                 3626GTS            OK                    OK
3                 3626GTS-PWR+       OK                    OK
 -------------------------------------------------------------------------------
Switch Units Found = 3
Stack Health Check = OK - RESILIENT
Stack Diagnosis = Stack in full resilient mode.
```

The following figure provides a sample of the **`show stack health`** command after unit 1 is turned off.

```
Switch#show stack health

--------------------------------------------------------------------------------
UNIT#            Switch Model       Cascade Up            Cascade Down
--------------------------------------------------------------------------------
```

```
2 (Temporary Base)3626GTS            LINK DOWN or MISSING  OK
3                 3626GTS-PWR+       LINK DOWN or MISSING  OK
 --------------------------------------------------------------------------------
Switch Units Found = 2
Stack Health Check = WARNING - NON-RESILIENT WITH TEMPORARY BASE
Stack Diagnosis = Stack in non-resilient mode, with temporary base unit.
Recommend replacing failed base unit or to add/replace the identified cables.
```

Displaying stack monitor information

Use this procedure to display the current values for the stack monitor.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show stack-monitor
   ```

Example

The following figure provides a sample of the **`show stack-monitor`** command.

```
Switch#show stack-monitor
Status: enabled
Stack size: 3
Trap interval: 60
```

Configuring the stack monitor

Use this procedure to configure the values for the stack monitor.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

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

Example

The following figure provides a sample of the **`stack-monitor`** command.

```
Switch(config)#stack-monitor enable stack-size 3 trap-interval 60
```

Variable definitions

The following table describes the parameters for the **`stack-monitor`** command.

Variable	Value
enable	Enables stack monitoring
stack-size <*2–8*>	Specifies the stack size to be monitored RANGE: 2 to 8 units DEFAULT: 2
trap-interval <*30–300*>	Specifies the interval between traps RANGE: 30 to 300 seconds DEFAULT: 60 seconds

Disabling the stack monitor

Use this procedure to disable the stack monitor.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   no stack-monitor
   ```

Rebooting stack units on failure

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Displaying stack reboot on failure status

Use this procedure to view whether stack reboot on failure capability is enabled or disabled.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Example

The following figure provides a sample of the **show stack reboot-on-failure** command.

```
Switch#show stack reboot-on-failure
Stack Reboot on Failure:  Enabled
```

Disabling stack reboot on failure

Use this procedure to disable stack reboot on failure. If this feature is disabled the system does not reboot stack units when it detects failure on stacking ports.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Configuring stack retry count

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   stack retry-count [retry-count]
   ```

Example

The following figure provides a sample of the **stack retry-count** command.

```
Switch(config)#stack retry-count 5
```

Variable definitions

The following table describes the parameters for the **stack retry-count** command.

Variable	Value
retry count *<0–4294967295>*	Sets the retry count for the stack. RANGE: 0 to 4294967295 DEFAULT: 0 **Note:** To use the command, you must enter a value.

Displaying stack retry count

Use this procedure to display the current stack retry count value. This value represents the number of times the system attempts to reach a unit before it indicates that the unit is down.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show stack retry-count
   ```

Example

The following figure provides a sample of the **`show stack retry-count`** command.

```
Switch#show stack retry-count
Stack Retry Count:  5
```

Displaying unit stack uptime

Use this procedure to display stack uptime for each unit in the stack.

Procedure

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

   ```
   show stack-info uptime
   ```

Example

The following figure provides a sample of the **`show stack-info uptime`** command.

```
switch#show stack-info uptime
Unit# Switch Model     Unit UpTime
----- ---------------- -------------------
1     3626GTS          0 days, 00:04:20
2     3626GTS          0 days, 00:04:04
3     3626GTS-PWR+     0 days, 00:04:02
```

Displaying environmental status

Use this procedure to view the environmental status of the switch or stack.

Procedure

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

   ```
   show environmental
   ```

   Note:

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

Example

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

```
Switch>show environmental
Unit# FAN1 FAN2 FAN3 FAN4 Temperature
----- ---- ---- ---- ---- -----------
1     OK   N/A  N/A  N/A   OK   39.5C
```

Displaying environmental status

Use this procedure to view the environmental status of the switch or stack.

Procedure

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

   ```
   show environmental
   ```

   Note:

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

Example

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

```
Switch>show environmental
Unit# FAN1 FAN2 FAN3 FAN4 Temperature
----- ---- ---- ---- ---- -----------
1     OK   N/A  N/A  N/A   OK   39.5C
```

System Monitoring Configuration using Enterprise Device Manager

This chapter describes how to use Enterprise Device Manager (EDM) to configure system logging and to display chassis and port statistics for the switch.

Displaying CPU and memory utilization using EDM

Use this procedure to view both CPU and memory utilization.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.

3. In the Chassis tree. double-click **Chassis**.
4. In the work area, click the **CPU/Mem Utilization** tab to display a table of CPU and memory utilization information for a switch or for all units of a stack.
5. On the toolbar, click **Refresh** to update the data.

CPU/Mem Utilization tab field descriptions

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

Name	Description
Unit	Displays the numerical representation of the unit
Last10Seconds	Displays CPU usage, in percentage, for the last 10 seconds
Last1Minute	Displays CPU usage, in percentage, for the last minute
Last10minutes	Displays CPU usage, in percentage, for the last 10 minutes
Last1hour	Displays CPU usage, in percentage, for the last hour
Last24Hours	Displays CPU usage, in percentage, for the last 24 hours
TotalCPUUsage	Displays the CPU load in percentage since the boot
MemoryTotalMB	Displays total memory present, in megabytes, on the unit
MemoryAvailableMB	Displays memory remaining available on the unit
MemoryUsedMB	Displays memory that has been used on the unit

Switch stack information configuration

This section describes procedures you can use to observe and configure information about the switch stack.

Displaying stack information

Use this procedure to view the stack information to see a description of the units that are on the stack.

Procedure

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

Stack info field descriptions

The following table describes the fields on the Stack Info tab.

Name	Description
Indx	Indicates the line number for stack information.
Descr	Describes the component or subcomponent. If not available, the value is a zero length string.
Location	Indicates the geographic location of a component in a system modeled as a chassis, but possibly physically implemented with geographically separate devices connected to exchange management information. Chassis modeled in this manner are sometimes referred to as virtual chassis. An example value is: 4th flr wiring closet in big A. **Important:** This field applies only to components that are in either the Board or Unit groups. If the information is unavailable, for example, the chassis is not modeling a virtual chassis or component is not in a Board or Unit group, the value is a zero-length string. If this field is applicable and is not assigned a value through an SNMP SET PDU when the row is created, the value defaults to the value of the object `s5ChasComSerNum`.
LstChng	Indicates the value of sysUpTime when it was detected that the component or subcomponent was added to the chassis. If this action has no occurred since the cold or warm start of the agent, the value is zero.
AdminState	Indicates the state of the component or subcomponent: • **enable**: enables operation • **reset**: resets component
OperState	Indicates the current operational state of the component. The possible values are: • **other**: another state • **notAvail**: state not available • **removed**: component removed • **disabled**: operation disabled • **normal**: normal operation • **resetInProg**: reset in progress

Table continues…

Name	Description
	• **testing**: performing a self test • **warning**: operating at warning level • **nonFatalErr**: operating at error level • **fatalErr**: error stopped operation The component type determines the allowable (and meaningful) values.
Ver	Indicates the version number of the component or subcomponent. If not available, the value is a zero-length string.
SerNum	Indicates the serial number of the component or subcomponent. If not available, the value is a zero-length string.
BaseNumPorts	Indicates the number of base ports of the component or subcomponent.
TotalNumPorts	Indicates the number of ports of the component or subcomponent.
IpAddress	Indicates the IP address of the component or subcomponent.
Ipv6Address	Specifies the IPv6 address of the component or subcomponent.
Ipv6NetMask	Specifies the IPv6 netmask of the component or subcomponent.
RunningSoftwareVer	Indicates the software version running on the switch.

Editing stack information

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

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Switch/Stack**.
4. In the work area, click the **Stack info** tab to display the current stack information.
5. Double-click a location in a unit description to change the name of the location.
6. Type the name of the new location.
7. Double-click the Admin State in a unit description.

   An arrow appears in the cell.
8. Click the arrow.

   A box appears with two options: enable and reset.

9. Click **enable** or **reset**.
10. On the toolbar, click **Apply**.
11. On the toolbar, you can click **Refresh** to verify the Admin State of a unit.

Stack info field descriptions

The following table describes the fields on the Stack info tab.

Name	Description
Location	Indicates the geographic location of a component in a system modeled as a chassis, but possibly physically implemented with geographically separate devices connected to exchange management information. Chassis modeled in this manner are sometimes referred to as virtual chassis. An example value is: 4th flr wiring closet in big A. **Important:** This field applies only to components that are in either the Board or Unit groups. If the information is unavailable, for example, the chassis is not modeling a virtual chassis or component is not in a Board or Unit group, the value is a zero-length string. If this field is applicable and is not assigned a value through an SNMP SET PDU when the row is created, the value defaults to the value of the object `s5ChasComSerNum`.
AdminState	Indicates the state of the component or subcomponent: • **enable**: enables operation • **reset**: resets component

Displaying pluggable ports

Use this procedure to view information about the pluggable ports.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, double-click **Switch/Stack**.
4. In the work area, click the **Stack info** tab to display the current stack information.
5. On the toolbar, click **Pluggable Ports**.
6. Observe the displayed information.

Stack info field descriptions

The following table describes the fields on the Stack info tab.

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

Displaying stack health

Use this procedure to view stack health information and statistics.

Procedure

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

Stack Health field descriptions

The following table describes the fields on the Stack Health tab.

Name	Description
Switch Units Found	Indicates the number of switch units in the stack DEFAULT: 2 RANGE: 2 to 8 units
Stack Health Check	Indicates the stack health
Stack Diagnosis	Indicates the stack mode

Displaying switch power supply information using EDM

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

Procedure

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

PowerSupply tab field descriptions

The following table describes the fields on the PowerSupply tab.

Name	Description
Unit	Displays the switch.
Primary Power Supply	Displays the power status for the switch, or for each unit in a stack.

Displaying switch fan information using EDM

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

Procedure

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

Fan tab field descriptions

The following table describes the fields on the Fan tab.

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

Note:

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

Displaying switch temperature using EDM

Use this procedure to display switch temperature information.

Procedure

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

Temperature tab field descriptions

The following table describes the fields on the Temperature tab.

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

Configuring remote system logging using EDM

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

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics tree, click **System Log**.
4. In the work area, click the **Remote System Log** tab to display the Remote System Log Information.
5. In the **RemoteSyslogAddressType** field, choose the type of IP address for the primary remote system log server.
6. In the **RemoteSyslogAddress** box, enter the IP address for the primary remote system log server.

7. OPTIONAL: In the **SecondarySyslogAddressType** field, choose the type of IP address for the secondary remote system log server.
8. OPTIONAL: In the **SecondarySyslogAddress** box, enter the IP address for the secondary remote system log server.
9. Do one of the following:
   - Select the **Enabled** check box to enable remote system logging.
   - Clear the **Enabled** check box to disable remote system logging.
10. In the **Save Targets** box, select the types of messages you want the system to report to the remote system log server or servers (if you are using Dual Syslog Servers).
11. In the **Facility** box, specify the remote logging facility.
12. On the toolbar, click **Apply**.

Remote System Log tab field descriptions

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

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

Table continues…

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

Displaying system log settings using EDM

Use this procedure to view System Log Settings information.

Procedure

1. In the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Diagnostics**.
3. In the **Diagnostics** tree, double-click **System Log**.
4. In the work area, click the **System Log Settings** tab to display the system log settings.

System Log Settings tab field descriptions

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

Name	Description
Operation	Enables you store or discard generated log messages. When you specify **on**, the system stores log messages in the log message buffer facility according to the parameters specified by related management objects. When you specify **off,** the system discontinues log message accumulation. **Important:** This does not affect operation of the remote syslog facility; it only determines whether log messages are stored locally.

Table continues…

Name	Description
BufferFullAction	Specifies the action to take when buffer space is exhausted. **Overwrite** causes the previous messages to be overwritten. Messages are overwritten based on First in First Out (FIFO). Specifying **latch** causes no more messages to be saved until this object is changed to overwrite or until the buffer space is made available through some other means (for example, clearing the buffer).
Volatile —CurSize	Displays the current number of log messages in the volatile portion of the system log messages facility. Messages that are classified as volatile are lost upon system reinitialization.
Volatile —SaveTargets	Determines the type of log messages that are saved in the log message buffer facilities. Messages are classified based on their type as follows: • critical • critical/serious • critical/serious/inform • none Selecting the type causes all log messages with an associated value less than or equal to the type value specified to be saved after the log message is entered in the system. For example, specifying the value critical causes only messages classified as critical to be saved to nonvolatile storage. Specifying critical/serious causes critical and serious messages to be saved. Specifying a value of none means no log messages are stored in volatile memory.
non-Volatile —CurSize	Displays the current number of log messages that are present in the nonvolatile portion of the system log message facility. Messages that are classified as nonvolatile are saved across system reinitilizations.
non-Volatile —SaveTargets	Determines the type of log messages that are saved to nonvolatile storage after they occur. Messages are classified based on their type as follows: • critical • critical/serious

Table continues…

Name	Description
	• none When you select a value the system saves all log messages with a value less than or equal to the specified value when the log message is entered in the system. For example, specifying the value critical causes only messages classified as critical to be saved to nonvolatile storage. Specifying critical/serious causes critical and serious messages to be saved. Specifying a value of none means no log messages are stored in volatile memory.
Action — ClearMessageBuffers	Indicates that the messages currently saved in the log message buffer that match the specified type are to be deleted. All messages of types matching the specified bits are deleted. For example, specifying volInformational deletes all informational messages and specifying nonVolCritical deletes all critical messages from nonvolatile storage.

Displaying system logs using EDM

Use this procedure to view System Logs information.

Procedure

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

System Logs tab field descriptions

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

Name	Description
OrigUnitNumber	Specifies the unit number of the originator of the log message.
MsgTime	Specifies the time (in hundredths of a second) between system initialization and the time this log message was entered into the system.
MsgIndex	Specifies the arbitrary integer index assigned to the log message upon entry into the message facility.

Table continues…

Name	Description
MsgSrc	Specifies the message source that indicates whether this message is loaded from nonvolatile storage at system initialization or whether the message is generated after that time.
MsgString	Specifies a printable string indicating the originator of and the reason why a log message is generated. This string, coupled with the log message parameters that are associated with the message, provides an understanding of the log message.
MsgType	Specifies the type of system message.

Displaying network topology information using EDM

Use this procedure to display network topology information.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, click **Diagnostics**.
3. In the Diagnostics work area, click the **Topology** tab.
4. In the Status section, configure as required.
5. On the toolbar, click **Apply**.

Variable definitions

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

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

Displaying the topology table using EDM

Use this procedure to display the topology table.

Procedure

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

Variable definitions

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

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

Port Mirroring using EDM

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

Displaying Port Mirroring using EDM

Use this procedure to troubleshoot the network.

Procedure

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

Port Mirrors tab field descriptions

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

Name	Description
Instance	Indicates the Port Mirroring instance number.
PortMode	Indicates the supported Port Mirroring modes. The modes are: • **manytoOneRx**— Many to one port mirroring on ingress packets. • **manytoOneRxTx**— Many to one port mirroring on ingress & egress traffic. • **manytoOneTx** — Many to one port mirroring on egress traffic. • **Xrx**— monitors all traffic received on port **X**. • **XrxOrXtx**— monitors all traffic received or transmitted on port **X**. • **XrxOrYtx** — monitors all traffic received on port **X** or transmitted by **Y**. • **Xtx** — monitors all traffic transmitted on port **X**.
MonitorPort	Indicates the switch port to designate as the monitor port.
PortListX	Indicates the switch port to be monitored by the designated monitor port. This port is monitored according to the value **X** in the Monitoring Mode field.

Configuring Port Mirroring using EDM

Use this procedure to help you troubleshoot the network.

Procedure

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

   The **Insert Port Mirrors** dialog box appears.
5. In the **instance** box, type the instance number.
6. In the **PortMode** section, click a mode.
7. Beside the **MonitorPort** box, click the ellipsis (...).
8. In the **Port Editor: MonitorPort** list, click a monitor port.
9. Click **Ok**.
10. In the **PortListX** box, click the ellipsis (…).
11. In the **Port Editor: PortListX** list, click a port, ports, or All to add to the list.
12. Click **Ok**.
13. Click **Insert**.

Port Mirrors tab field descriptions

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

Name	Description
Instance	Specifies the Port Mirroring instance number.
PortMode	Specifies the supported Port Mirroring modes. The modes are: • **manytoOneRx** — Many to one port mirroring on ingress packets. • **manytoOneRxTx** — Many to one port mirroring on ingress and egress traffic. • **manytoOneTx** — Many to one port mirroring on egress packets. • **Xrx**— monitors all traffic received on port **X**. • **XrxOrXtx**— monitors all traffic received or transmitted on port **X**. • **XrxOrYtx** — monitors packets received on port **X** or transmitted on port **Y**. • **Xtx** — monitors all traffic transmitted on port **X**.

Table continues…

Name	Description
MonitorPort	Specifies the switch port to designate as the monitor port.
PortListX	Specifies the switch port to be monitored by the designated monitor port. This port is monitored according to the value **X** in the Monitoring Mode field.

Graphing chassis statistics using EDM

Use this procedure to graph chassis statistics.

Procedure

1. In the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**. The **Graph Chassis** dialog box appears with the **SNMP** tab displayed.
3. Click a row of data to graph under a column heading.
4. On the toolbar, click the **Poll Interval** and select an interval.
5. On the toolbar, you can reset the data by clicking **Clear Counters**.
6. On the toolbar, click a graph type.

Displaying IP statistics using EDM

Use this procedure to view and graph IP statistics.

Procedure

1. In the navigation tree, double-click **Graph**.
2. in the Graph tree, double-click **Chassis**.
3. In the work area, click the **IP** tab.
4. Click a row of data to graph under a column heading.
5. On the toolbar, click the **Poll Interval** and select an interval.
6. On the toolbar, you can reset the data by clicking **Clear Counters**.
7. On the toolbar, click a graph type to graph the IP statistics.

IP tab field descriptions

The following table describes the fields on the IP tab.

Name	Description
InReceives	Specifies the total number of input datagrams received from interfaces, including those received in error.
InHdrErrors	Specifies the number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options.
InAddrErrors	Specifies the number of input datagrams discarded because the IP address in the IP header destination field was not a valid address. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For addresses that are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ForwDatagrams	Specifies the number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. For addresses that do not act as IP Gateways, this counter includes only those packets Source-Routed by way of this address with successful Source-Route option processing.
InUnknownProtos	Specifies the number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InDiscards	Specifies the number of input IP datagrams for which no problems are encountered to prevent their continued processing, but that are discarded (for example, for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.
InDelivers	Specifies the total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	Specifies the total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in ipForwDatagrams.
OutDiscards	Specifies the number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that are discarded (for example, for lack of buffer space).

Table continues…

Name	Description
	This counter can include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
OutNoRoutes	Specifies the number of IP datagrams discarded because no route can be found to transmit them to their destination. This counter also includes any packets counted in ipForwDatagrams that have no route. This includes any datagrams a host cannot route because all of its default gateways are down.
FragOKs	Specifies the number of IP datagrams successfully fragmented at this entity.
FragFails	Specifies the number of IP datagrams that are discarded because they need to be fragmented at this entity but cannot be, for example, because their Don't Fragment flag was set.
FragCreates	Specifies the number of generated IP datagram fragments because of a fragmentation at this entity.
ReasmReqds	Specifies the number of IP fragments received that needed to be reassembled at this entity.
ReasmOKs	Specifies the number of IP datagrams successfully reassembled.
ReasmFails	Specifies the number of failures detected by the IP reassembly algorithm (for example, timed out, errors). This is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC815) can lose track of the number of fragments by combining them as they are received.

Displaying ICMP In statistics using EDM

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

Procedure

1. In the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **ICMP In** tab.
4. Click the row of data to graph under a column heading.
5. On the toolbar, click the **Poll Interval** and select an interval.
6. On the toolbar, you can reset the data by clicking **Clear Counters**.
7. On the toolbar, click a graph type.

ICMP Intab field descriptions

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

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

Displaying ICMP Out statistics using EDM

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

Procedure

1. In the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **ICMP Out** tab.
4. Click the row of data to graph under a column heading.
5. On the toolbar, click the **Poll Interval** and select an interval.
6. On the toolbar, you can reset the data by clicking **Clear Counters**.
7. On the toolbar, click a graph type.

ICMP Out tab field descriptions

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

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

Displaying TCP statistics using EDM

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

Procedure

1. In the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **TCP** tab.
4. Click the row of data to graph under a column heading.
5. On the toolbar, click the **Poll Interval** and select an interval.
6. On the toolbar, you can reset the data by clicking **Clear Counters**.
7. On the toolbar, click a graph type.

TCP tab field descriptions

The following table describes the fields on the TCP tab.

Name	Description
ActiveOpens	Displays the number of times TCP connections make a direct transition to the SYN-SENT state from the CLOSED state.
PassiveOpens	Displays the number of times TCP connections make a direct transition to the SYN-RCVD state from the LISTEN state.
AttemptFails	Displays the number of times TCP connections make a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections make a direct transition to the LISTEN state from the SYNRCVD state.
EstabResets	Displays the number of times TCP connections make a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
CurrEstab	Displays the number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
InSegs	Displays the total number of segments received, including those received in error. This count includes segments received on currently established connections.
OutSegs	Displays the total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
ReTransSegs	Displays the total number of segments retransmitted, that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
InErrs	Displays the total number of segments received in error (for example, bad TCP checksums).
OutRsts	Displays the number of TCP segments sent containing the RST flag.
HcInSegs	Displays the number of segments received, including those received in error. This count includes segments received on currently established connections. This object is the 64-bit equivalent of InSegs.
HCOutSegs	Displays the number of segments sent, including those on current connections, but excluding those containing only retransmitted octets. This object is the 64-bit equivalent of OutSegs.

Displaying UDP statistics using EDM

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

Procedure

1. In the navigation tree, double-click **Graph**.
2. In the Graph tree, double-click **Chassis**.
3. In the work area, click the **UDP** tab.
4. Click the row of data to graph under a column heading.
5. On the toolbar, click the **Poll Interval** and select an interval.
6. On the toolbar, you can reset the data by clicking **Clear Counters**.
7. On the toolbar, click a graph type.

UDP tab field descriptions

The following table describes the fields on the UDP tab.

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

Note:

HC counters are 64 bits (versus the standard 32 bit counters). The maximum is 18,446,744,073,709,551,613 before rolling over.

Displaying port statistics using EDM

You can graph the following types of statistics for a port:

- AbsoluteValue
- Cumulative
- Average/sec
- Minimum/sec
- Maximum/sec
- LastVal/sec

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

Procedure

1. On the Device Physical View, click on the port you want to graph.
2. In the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the tab for the data type you want to view and graph.
5. Click a row of data to graph under a column heading.
6. On the toolbar, click the **Poll Interval** and select an interval.
7. On the toolbar, you can reset the data by clicking **Clear Counters**.
8. On the toolbar, click a graph type.

Graphing interface statistics

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

Procedure

1. On the Device Physical View, click on a port.
2. In the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **Interface** tab.
5. Click a row of data to graph under a column heading.
6. On the toolbar, click the **Poll Interval** and select an interval.
7. On the toolbar, you can reset the data by clicking **Clear Counters**.
8. On the toolbar, click a graph type.

Interface tab field descriptions

The following table describes the fields on the Interface tab.

Name	Description
InOctets	Displays the total number of octets received on the interface, including framing characters.
OutOctets	Displays the total number of octets transmitted out of the interface, including framing characters.
InUcastPkts	Displays the number of packets delivered by this sublayer to a higher sublayer that are not addressed to a multicast or broadcast address at this sublayer.
OutNUcastPkts	Displays the total number of packets that higher-level protocols requested be transmitted, and that are addressed to a multicast or broadcast address at this sublayer, including those that are discarded or not sent.
InMulticastPkts	Displays the number of packets delivered by this sublayer to a higher sublayer that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both group and functional addresses.
OutMulticastPkts	Displays the number of packets that higher-level protocols requested be transmitted, and that are addressed to a multicast address at this sublayer, including those that were discarded or not sent. For a MAC layer protocol, this number includes both group and functional addresses.
InBroadcastPkts	Displays the number of packets delivered by this sublayer to a higher sublayer that are addressed to a broadcast address at this sublayer.
OutBroadcastPkts	Displays the number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this sublayer, including those that were discarded or not sent.
InDiscards	Displays the number of inbound packets chosen to be discarded even though no errors were detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet can be to free up buffer space.
OutDiscards	Displays the number of outbound packets chosen to be discarded even though no errors were detected to prevent them from being transmitted. One possible reason for discarding such a packet can be to free up buffer space.
InErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length

Table continues…

Name	Description
	interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
OutErrors	For packet-oriented interfaces, the number of outbound packets that cannot be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that cannot be transmitted because of errors.
InUnknownProtos	For packet-oriented interfaces, the number of packets received through the interface that are discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received through the interface that are discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter is always zero.

Graphing Ethernet error statistics using EDM

Use this procedure to view and graph Ethernet error statistics.

Procedure

1. On the Device Physical View, click on a port.
2. In the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **Ethernet Errors** tab.
5. Click a row of data to graph under a column heading.
6. On the toolbar, click the **Poll Interval** and select an interval.
7. On the toolbar, you can reset the data by clicking **Clear Counters**.
8. On the toolbar, click a graph type.

Ethernet Errors tab field descriptions

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

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

Table continues…

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

Table continues…

Name	Description
	other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
SQETestErrors	Specifies a count of times that the SQE Test Errors message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/ IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
DeferredTransmissions	Specifies a count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollisionFrames	Specifies a count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object.
MultipleCollisionFrames	Specifies a count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	Specifies the number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
ExcessiveCollisions	Specifies a count of frames for which transmission on a particular interface fails due to excessive collisions.

Graphing miscellaneous statistics using EDM

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

Procedure

1. On the Device Physical View, click on a port.
2. In the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **Misc. Stats** tab.
5. Click a row of data to graph under a column heading.
6. On the toolbar, click the **Poll Interval** and select an interval.
7. On the toolbar, you can reset the data by clicking **Clear Counters**.
8. On the toolbar, click a graph type.

Misc. Stats tab field descriptions

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

Name	Description
NoResourcesPktsDropped	Displays the number of packets dropped due to switch packet buffer full.

Configuring the stack monitor

Use this procedure to specify the stack parameters to be monitored using EDM.

Procedure

1. From the navigation tree, double-click **Edit**.
2. In the Edit tree, double-click **Chassis**.
3. In the Chassis tree, click **Chassis**.
4. In the work area, click the **Stack Monitor** tab.
5. Configure the stack monitor parameters as required.
6. On the toolbar, click **Apply**.
7. On the toolbar you can click **Refresh** to verify the stack monitor configuration.

Stack Monitor field descriptions

The following table describes the fields on the Stack Monitor tab.

Name	Description
StackErrorNotificationEnabled	Enables or disables stack monitoring DEFAULT: Disabled
ExpectedStackSize	Specifies stack size to be monitored DEFAULT: 2 RANGE: 2 to 8
StackErrorNotificationInterval	Specifies the interval between traps in seconds DEFAULT: 60 seconds RANGE: 30 to 300 seconds

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

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

Procedure

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

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

Using the EDM MIB Web page for SNMP walk

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

Procedure

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

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

Chapter 4: Remote Monitoring

This chapter provides conceptual information and procedures to configure Remote Monitoring.

Remote Monitoring fundamentals

Remote monitoring (RMON) MIB is an interface between the RMON agent on a switch and an RMON management application, such as Enterprise Device Manager.

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

The RMON agent continuously collects statistics and proactively monitors switch performance. You can view this data through CLI and EDM.

RMON has three major functions:

- creating and displaying alarms for user-defined events
- gathering cumulative statistics for Ethernet interfaces
- tracking a history of statistics for Ethernet interfaces

RMON alarms

Alarms are useful when you need to know when the values of a variable go out of range. You can define an RMON alarm for any MIB variable that resolves to an integer value. You cannot use string variables (such as system description) as alarm variables.

All alarms share the following characteristics:

- An upper and lower threshold value is defined.
- A corresponding rising and falling event occurs.
- An alarm interval or polling period is reached. When alarms are activated, you can view the activity in a log or a trap log, or you can create a script to notify you by sending an audible sound to a console, sending e-mail, or calling a pager.

How RMON alarms work

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

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

During the first interval in which the data drops below the falling value, the alarm triggers as a falling event.

The following figure describes how alarms are triggered.

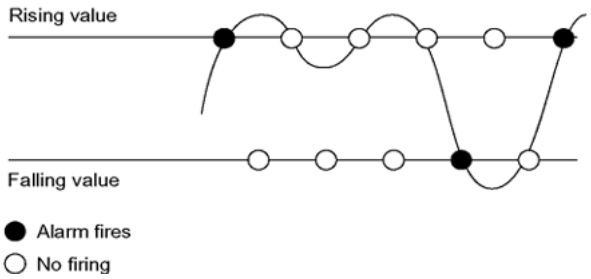


Figure 1: RMON alarm triggers

The alarm fires during the first interval that the sample goes out of range. No additional events are generated for that threshold until the opposite threshold is crossed. Therefore, it is important to carefully define the rising and falling threshold values for alarms to work as expected. Otherwise, incorrect thresholds cause an alarm to fire at every alarm interval.

A general guideline is to define one of the threshold values to an expected baseline value, and then define the opposite threshold as the out-of-bounds limit. Because of sample averaging, the value may be equal to ±1 of the baseline units. For example, assume an alarm is defined on octets going out of a port as the variable. The intent of the alarm is to provide notification to you after excessive traffic occurs on that port. If spanning tree is enabled, 52 octets are transmitted out of the port every 2 seconds, which is equivalent to baseline traffic of 260 octets every 10 seconds. This alarm provides notification to you if the lower limit of octets going out is defined at 260 and the upper limit is defined at 320 (or at a value greater than 260 + 52 = 312).

The first time outbound traffic other than spanning tree Bridge Protocol Data Units (BPDU) occurs, the rising alarm fires. After outbound traffic other than spanning tree ceases, the falling alarm fires. This process provides you with time intervals of a non-baseline outbound traffic.

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

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

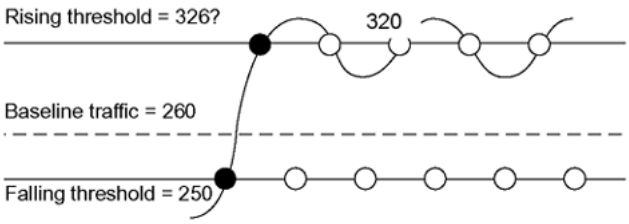


Figure 2: RMON alarm thresholds

Creating alarms

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

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

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

How events work

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

- Rising Event
- Falling Event

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

RMON Configuration using the CLI

Use the procedures in this section to configure Remote Monitoring (RMON), using the CLI.

Displaying RMON alarms

Displays information about RMON alarms.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show rmon alarm
   ```

Displaying the RMON events

Displays information about RMON events.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   show rmon event
   ```

Displaying RMON history

Displays information about RMON events

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   show rmon history
   ```

Displaying RMON statistics

Displays information about the configuration of RMON statistics

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   show rmon stats
   ```

Displaying RMON history for a port

Displays RMON history for a port.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   show rmon ethernet history port [LINE]
   ```

Variable definitions

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

Variable	Value
LINE	Specifies a list of ports

Displaying RMON packets for a port

Display RMON packets for all ports or specific ports.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   show rmon ethernet packets [port <LINE>]
   ```

Variable definitions

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

Variable	Value
LINE	Specifies a list of ports

Displaying RMON statistics for a port

Displays RMON statistics for all or specific ports.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   show rmon ethernet statistics [port <LINE>]
   ```

Variable definitions

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

Variable	Value
LINE	Specifies a list of ports

Configuring RMON Alarms

Set RMON alarms and thresholds.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

Variable	Value
<1–65535>	Specifies the unique index for the alarm entry
<WORD>	Specifies the MIB object to be monitored. This is an object identifier, and for most available objects, an English name can be used
<1–2147483647>	Specifies the sampling interval, in seconds
absolute	Specifies absolute values (value of the MIB object is compared directly with thresholds)
delta	Specifies delta values (change in the value of the MIB object between samples is compared with thresholds)
rising-threshold*<-2147483648–2147483647 > [<1–65535>]*	Specifies the first integer value is the rising threshold value. The optional second integer specifies the event entry to be triggered when the rising threshold is crossed. If omitted, or if an invalid event entry is referenced, no event is triggered. Unique index for the alarm entry
falling-threshold*<-2147483648–2147483647 > [<1–65535>]*	Specifies the first integer value is the falling threshold value. The optional second integer specifies the event entry to be triggered when the falling threshold is crossed. If omitted, or if an invalid event entry is referenced, no event is triggered. Unique index for the alarm entry.
[owner <LINE>]	Specifies the owner string to identify the alarm entry

Deleting RMON alarms using CLI

To delete RMON alarm table entries.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Configuring RMON events settings

Configure RMON event log and trap settings.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   [no] rmon event <1–65535> [log] [trap] [description <LINE>] [owner <LINE>]
   ```

Variable definitions

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

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

Configuring RMON History Settings

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Configuring RMON statistics settings

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Displaying environmental status

Use this procedure to view the environmental status of the switch or stack.

Procedure

1. Log on to CLI to enter User EXEC mode.

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

   ```
   show environmental
   ```

   Note:

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

Example

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

```
Switch>show environmental
Unit# FAN1 FAN2 FAN3 FAN4 Temperature
----- ---- ---- ---- ---- -----------
1     OK   N/A  N/A  N/A   OK   39.5C
```

RMON using Enterprise Device Manager

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

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

The RMON agent continuously collects statistics and monitors switch performance. You can view this data through EDM.

RMON has three major functions:

- creating and displaying alarms for user-defined events
- gathering cumulative statistics for Ethernet interfaces
- tracking a history of statistics for Ethernet interfaces

Working with RMON information:

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

Displaying RMON statistics using EDM

You can use EDM to gather Ethernet statistics that you can graph in a variety of formats. You can save the statistics output to a file and export the statistics to an outside presentation or graphing application.

The following types of RMON statistics are available:

- Absolute — The total count since the last time counters were reset. A system restart resets all counters

- Cumulative — The total count since the statistics tab was first opened. The elapsed time for the cumulative counter appears at the bottom of the graph window.
- Average/sec — The cumulative count divided by the cumulative elapsed time.
- Min/sec — The minimum average for the counter for a given polling interval over the cumulative elapsed time.
- Max/sec — The maximum average for the counter for a given polling interval over the cumulative elapsed time.
- Last/Val/sec — The average for the counter over the last polling interval.

Perform this procedure to view RMON Ethernet statistics.

Procedure

1. On the Device Physical View, lick on a port.
2. In the navigation tree, double-click **Graph**.
3. In the Graph tree, double-click **Port**.
4. In the work area, click the **RMON** tab.
5. Click the row of data to graph under a column heading.
6. On the toolbar, click the **Poll Interval** and select an interval.
7. On the toolbar, you can reset the data by clicking **Clear Counters**.
8. On the toolbar, click a graph type.

RMON tab field descriptions

The following table describes the fields on the RMON tab.

Name	Description
Octets	Displays the total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval.
Pkts	Displays the total number of packets (including bad packets, broadcast packets, and multicast packets) received.
BroadcastPkts	Displays the total number of good packets received that are directed to the broadcast address. This does not include multicast packets.
MulticastPkts	Displays the total number of good packets received that are directed to a multicast address. This number

Table continues…

Name	Description
	does not include packets directed to the broadcast address.
CRCAlignErrors	Displays the total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
UndersizePkts	Displays the total number of packets received that are less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
Fragments	Displays the total number of packets received that are less than 64 octets in length (excluding framing bits but including FCS octets) and with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). For etherStatsFragments to increment is normal because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Collisions	Displays the best estimate of the total number of collisions on this Ethernet segment.
Jabbers	Displays the total number of packets received that are longer than 1518 octets (excluding framing bits, but including FCS octets), with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
1 to 64	Displays the total number of packets (including bad packets) received that are less than or equal to 64 octets in length (excluding framing bits but including FCS octets).
65 to 127	Displays the total number of packets (including bad packets) received that are greater than 64 octets in length (excluding framing bits but including FCS octets).
128 to 255	Displays the total number of packets (including bad packets) received that are greater than 127 octets in length (excluding framing bits but including FCS octets).
256 to 511	Displays the total number of packets (including bad packets) received that are greater than 255 octets in

Table continues…

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

Configuring the IPv4 remote access list using EDM

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

Procedure

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

Variable definitions

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

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

Configuring the IPv6 remote access list using EDM

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

Procedure

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

Variable definitions

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

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

RMON history management using EDM

Use the following procedures to manage RMON history.

Displaying RMON history using EDM

Ethernet history records periodic statistical samples from a network. A sample is called a history and is gathered in time intervals referred to as buckets. Histories establish a time-dependent method for gathering RMON statistics on a port. The default values for history are as follows:

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

You can configure both the time interval and the number of buckets. However, when the last bucket is reached, bucket 1 is dumped and recycled to hold a new bucket of statistics. Then subsequent buckets are dumped in numerical order.

Use this procedure to view RMON history.

Procedure

1. In the navigation tree, double-click **Rmon**.
2. In the RMON tree, double-click **Control**.

   The **Rmon Control** work area appears with the **History** tab displayed.

Creating RMON history characteristics using EDM

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

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

Before you begin

Procedure

1. In the navigation tree, double-click **Rmon**.
2. In the RMON tree, double-click **Control**.
3. In the work area, click **Insert** to open the Insert History dialog.
4. Type the port number or click the ellipsis to select a port from the list.
5. In the **Buckets Requested** box, type the number of buckets, or click the ellipsis to select a value from the list. The default value is 50.
6. In the **Interval** box, type the length of the interval or click the ellipsis to select a value from the list. The default value is 1800.
7. In the **Owner** box, type the owner — the network management system that created this entry.
8. Click **Insert** to add the entry to the list and return to the **History** tab.

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

RMON History tab field descriptions

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

Name	Description
Index	Specifies a unique value assigned to each interface. An index identifies an entry in a table.
Port	Specifies any Ethernet interface on the device.
BucketsRequested	Specifies the requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this entry.
BucketsGranted	Specifies the number of discrete sampling intervals over which data is saved in the part of the media-specific table associated with this entry. The actual number of buckets associated with this entry can be less than the value of this object. In this case, at the end of each sampling interval, a new bucket is added to the media-specific table.

Table continues…

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

Disabling RMON history using EDM

Use this procedure to disable RMON history on a port.

Procedure

1. In the navigation tree, double-click **Rmon**.
2. In the RMON tree, double-click **Control**.
3. In the work area, click the row that contains the port ID you want to delete.
4. Click **Delete**.
5. On the toolbar, click **Yes** to delete the data and return to the **History** tab, or click **No** to return to the **History** tab without deleting the data.

Graphing RMON history statistics using EDM

Use this procedure to display and graph RMON History statistics.

Procedure

1. In the navigation tree, double-click **Rmon**.
2. In the RMON tree, double-click **Control**.
3. In the work area, click a row of data to graph.
4. On the toolbar, click **Display History Data**.

Display History Data tab field descriptions

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

Name	Description
SampleIndex	Displays an index that uniquely identifies the particular sample this entry represents among all the samples associated with the same entry. This index starts at 1 and increases by one as each new sample is taken.
Utilization	Displays the best estimate of the mean physical layer network utilization on this interface during the sampling interval (in hundredths of a percent).
Octets	Displays the total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval.
Pkts	Displays the total number of packets (including bad packets, broadcast packets, and multicast packets) received.
BroadcastPkts	Displays the total number of good packets received that are directed to the broadcast address. This does not include multicast packets.
MulticastPkts	Displays the total number of good packets received that are directed to a multicast address. This number does not include packets directed to the broadcast address.
DropEvents	Displays the total number of events in which packets are dropped by the probe due to lack of resources during this sampling. This number is not necessarily the number of packets dropped; it is the number of times this condition is detected.
CRCAlignErrors	Displays the total number of packets received with a length (excluding framing bits, but including FCS octets) between 64 and 1518 octets, inclusive, but with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
UndersizePkts	Displays the total number of packets received that are less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.

Table continues…

Name	Description
OversizePkts	Displays the total number of packets received that are longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
Fragments	Displays the number of packets received during the sampling interval were less than 64 octets long (including FCS octets, but not framing bits. The packets had a bad FCS with either an integral number of octets (FCS Error), or a nonintegral number of octets (Alignment Error).
Collisions	Displays the best estimate of the number of collisions on an Ethernet segment during a sampling interval.

Ethernet statistics gathering using EDM

Use the following procedures to gather ethernet statistics using EDM.

Enabling Ethernet statistics gathering using EDM

Use this procedure to use RMON to gather Ethernet statistics.

Procedure

1. In the navigation tree, double-click **Rmon**.
2. In the Rmon tree, double-click **Control**.
3. In the work area, click the **Ether Stats** tab.
4. On the toolbar, click **Insert** to open the **Insert Ether Stats** dialog box.
5. In the **Index** box, type the index number of click the ellipsis (...) to select an index number from the list.

   After you enter the port number, EDM assigns an index number.
6. In the **Port** box, type the port number or click the ellipsis (...) to select a port from the list.
7. In the **Owner** box, type the owner information.
8. Click **Insert**.

Ether Stats tab field descriptions

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

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

Table continues…

Name	Description
Port	Specifies any Ethernet interface on the device.
Owner	Specifies the network management system which created this entity.

Disabling Ethernet statistics gathering using EDM

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

Procedure

1. In the navigation tree, double-click **Rmon**.
2. In the RMON tree, double-click **Control**.
3. In the work area, click the **Ether Stats** tab.
4. Click the row that contains the port ID you want to delete.
5. On the toolbar, click **Delete**.
6. Select **Yes** to delete the selected entry from the table, or click **No** to return to the **Ether Stats** tab without deleting the entry.

RMON alarm management using EDM

Use the following procedures to manage RMON alarms.

Creating an alarm using EDM

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

Procedure

1. In the navigation tree, double-click **Rmon**.
2. In the RMON tree, double-click **Alarms**.
3. On the toolbar, click **Insert** to open the **Insert Alarms** dialog box.
4. Type and select the values to create the alarm.
5. Click **Insert** to add the alarm and return to the **Alarms** tab.

Alarms tab field descriptions

The following table describes the fields on the Alarms tab.

Name	Description
Variable	Specifies the Name and Type of alarm in one of the following formats: • **alarm.x**: where x=0 to indicate a chassis alarm

Table continues…

Name	Description
	• **alarmname.**: where you specify the index. The index is a card number for module-related alarms, OR an STG ID for spanning tree group alarms (the default STG is 1, other STG IDs are user-configured), OR the Ether Statistics Control Index for RMON Stats alarms. • **alarmname with no dot or index**: is a port-related alarm and results in the display of the port selection tool.
Sample Type	Specifies either absolute or delta
Interval	Specifies the time period (in seconds) over which the data is sampled and compared with the rising and falling thresholds.
Index	Uniquely identifies an entry in the alarm table. Each entry defines a diagnostic sample at a particular interval for an object on the device.
Rising Threshold	Specifies that when the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, the alarm generates a single event.
RisingEventIndex	Specifies the index of the event entry that is used after a rising threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already entered.)
Falling Threshold	Specifies that when the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, the alarm generates a single event.
FallingEventIndex	Specifies the index of the event entry that is used after a falling threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already entered.)
Owner	Identifies the network management system which created this entry.

Deleting an alarm using EDM

Use this procedure to delete an alarm.

Procedure

1. In the navigation tree, double-click **Rmon**.

2. In the Rmon tree, double-click **Alarms**.
3. In the work area, click on a row for the alarm that you want to delete.
4. On the toolbar, click **Delete**.
5. Click **Yes** to delete the alarm and return to the **Alarms** tab, or click **No** to return to the **Alarms** tab without deleting the alarm.

Using RMON events

This section describes how RMON events and alarms work together to notify you after values in your network are outside of a specified range. When values pass the specified ranges, the alarm is triggered and it triggers. The event specifies how the activity is recorded.

Displaying an event using EDM

Use this procedure to view a table of events.

Procedure

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

Events tab field descriptions

The following table describes the fields on the Events tab.

Name	Description
Index	This index uniquely identifies an entry in the event table. Each entry defines one event that is to be generated after the appropriate conditions occur.
Description	Specifies whether the event is a rising or falling event.
Type	The type of notification that Enterprise Device Manager provides about this event. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations. Possible notifications are as follows: • none • log • trap • log-and-trap

Table continues…

Name	Description
Community	The SNMP community string acts as a password. Only those management applications with this community string can view the alarms.
LastTimeSent	The value of sysUpTime at the time this event entry last generated an event. If this entry has not generated any events, this value is zero.
Owner	If traps are specified to be set to the owner, this field specifies the name of the machine that receives alarm traps.

Creating an event using EDM

Use this procedure to create an event.

Procedure

1. In the navigation tree, double-click **Rmon**.
2. In the RMON tree, double-click **Alarms**.
3. In the work area, click the **Events** tab.
4. On the toolbar, click **Insert**.
5. In the **Index** box, type the index for the event.
6. In the **Description** box, type the description of the event.
7. In the **Type** section, click a type option button.

   To designate the event type to

   - save memory — specify the event type as **log**
   - reduce traffic from the switch or improve CPU utilization — specify the event type as **snmp-trap**

   Important:

   If you select an event type of **snmp-trap** or **log-and-trap**, you must set trap receivers.
8. In the **Community** box, type a community.
9. In the **Owner** box, type an owner.
10. Click **Insert**.

Deleting an event using EDM

Use this procedure to delete an event.

Procedure

1. In the navigation tree, double-click **Rmon**.
2. In the RMON tree, double-click **Alarms**.

3. In the work area, click the **Events** tab.
4. Click a row to delete.
5. On the toolbar, click **Delete**.
6. Click **Yes** to delete the event or click **No** to return to the **Events** tab.

Displaying RMON log information using EDM

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

Procedure

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

Log tab field descriptions

The following table describes the fields on the Log tab.

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

Chapter 5: Service Level Agreement Monitor

The switch supports the Service Level Agreement Monitor (SLA Mon) agent as part of the SLA Mon solution.

SLA Mon uses a server and agent relationship to perform end-to-end network Quality of Service (QoS) validation, and acts as a distributed monitoring device. You can use the test results to target under-performing areas of the network for deeper analysis.

Service Level Agreement Monitor fundamentals

This section contains information on the fundamental principles of the Service Level Agreement Monitor (SLA Mon).

SLA Mon Server and Agent

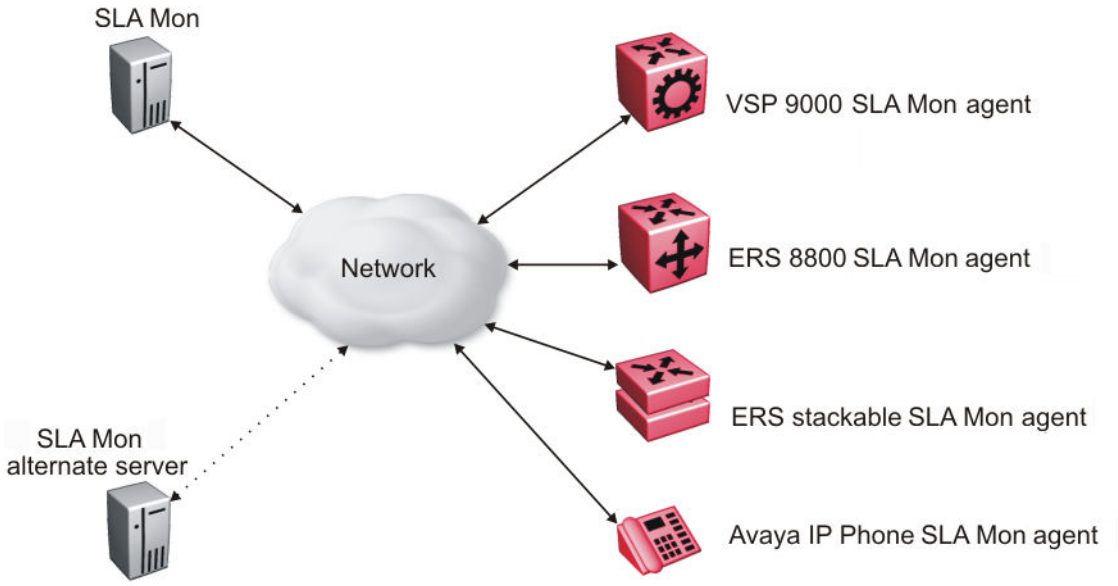
SLA Monitor agent performs QoS tests after it receives a request from the SLA Monitor server. The tests can be performed even if the server is not available.

The SLA Mon server initiates the SLA Mon functions on one or more agents, and the agents run specific QoS tests at the request of the server. Agents can exchange packets between one another to conduct the QoS tests.

SLA Monitor can monitor a number of key items, including the following:

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

The following figure illustrates an SLA Monitor implementation.



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

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

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

QoS Tests

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

- Real Time Protocol (RTP)

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

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

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

- You can access the SLA Monitor CLI through the SLAMon Agent Address and SLAMon Agent Port. By default, access to the SLA Monitor CLI interface is disabled. If access is enabled, the SLA Monitor CLI interface becomes available when the SLA Monitor agent is enabled. Tests are run serially and only one type of test can be run at a time. Established sessions time-out after a specified interval. The time interval can be 60 seconds to 600 seconds. By default, the

interval is 60 seconds. You can disable the SLA Monitor CLI interface if the functionality is not required.

- You can run the NTR and RTP tests through the CLI using the Application Configuration mode. The SLA Monitor agent must be enabled. Tests are run serially and only one type of test can be run at a time.

Note:

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

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

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

Note:

Command execution fails if you disable the SLA Monitor agent.

Limitations

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

SLA Monitor configuration using CLI

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

Displaying SLA Monitor agent settings

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display SLA Monitor agent settings:

   ```
   show application slamon agent
   ```

Example

```
Switch>enable
Switch#show application slamon agent

SLAMon Operational Mode: Disabled
SLAMon Agent Encryption: Supported
SLAMon Agent Address: 0.0.0.0
SLAMon Agent Port: 50011
SLAMon Agent Registration Status: Not Registered
SLAMon Registered Server Address: 0.0.0.0
SLAMon Registered Server Port: 0
SLAMon Server Registration Time: 0
SLAMon CLI Mode: Disabled
SLAMon CLI Timeout Mode: Enabled
SLAMon CLI Timeout: 60 seconds
SLAMon Configured Agent Address: 0.0.0.0
SLAMon Configured Agent Port: 0
SLAMon Configured Server Address: 0.0.0.0 0.0.0.0
SLAMon Configured Server Port: 0
SLAMon Agent-To-Agent Communication Port: 50012
SLAMon Configured Agent-To-Agent Communication Port: 0
SLAMon Agent Server Bypass: Disabled
SLAMon Agent Refuse Server Tests: Allow Tests
```

Configuring the SLA Monitor

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

Before you begin

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

About this task

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

Procedure

1. Enter Application Configuration mode:

   ```
   enable

   configure terminal

   application
   ```

2. Configure the agent IP address:

   ```
   slamon agent ip address {A.B.C.D}
   ```

3. Configure the agent IP address to its default value:

   ```
   default slamon agent ip address
   ```

4. Configure the UDP port:

```
slamon agent port <0, 1024-65535>
```

5. Configure the agent UDP port to its default value:

   ```
   default slamon agent port
   ```

6. Enable the agent:

   ```
   slamon oper-mode enable
   ```

7. Disable the agent:

   ```
   no slamon oper-mode [enable]
   ```

   OR

   ```
   default slamon oper-mode
   ```

8. Configure the agent-to-agent communication port:

   ```
   slamon agent—comm—port <0, 1024-65535>
   ```

9. Configure the agent-to-agent communication port to its default value:

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

10. Enable the SLA Monitor agent CLI support:

    ```
    slamon cli enable
    ```

    Note:

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

11. Disable the SLA Monitor agent CLI support:

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

    OR

    ```
    default slamon cli
    ```

12. Configure the agent automatic CLI session timeout value:

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

13. Enable the agent automatic CLI session timeout:

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

    OR

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

14. Disable the agent automatic CLI session timeout:

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

15. Configure the agent server IP address:

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

16. Configure the agent server IP address to its default value:

    ```
    default slamon server ip address
    ```

17. Configure the server TCP registration port:

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

18. Configure the server TCP registration port to its default value:

    ```
    default slamon server port
    ```

19. Enable the agent refuse server test mode:

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

20. Disable the agent refuse server test mode:

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

    OR

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

21. Enable the agent server bypass mode:

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

22. Disable the agent server bypass mode:

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

    OR

    ```
    default slamon server-bypass
    ```

23. Display the SLA monitor configuration:

    ```
    show application slamon agent
    ```

Example

```
Switch>enable
Switch#configure terminal
Switch(config)#application
Switch(config-app)#slamon oper-mode enable
Switch(config-app)#show application slamon agent

SLAMon Operational Mode: Enabled
SLAMon Agent Encryption: Not Supported
SLAMon Agent Address: 192.0.2.1
SLAMon Agent Port: 50011
SLAMon Agent Registration Status: Not Registered
SLAMon Registered Server Address: 0.0.0.0
SLAMon Registered Server Port: 0
SLAMon Server Registration Time: 0
SLAMon CLI Mode: Disabled
SLAMon CLI Timeout Mode: Enabled
SLAMon CLI Timeout: 60 seconds
SLAMon Configured Agent Address: 0.0.0.0
SLAMon Configured Agent Port: 0
SLAMon Configured Server Address: 0.0.0.0 0.0.0.0
SLAMon Configured Server Port: 0
SLAMon Agent-To-Agent Communication Port: 50012
```

```
SLAMon Configured Agent-To-Agent Communication Port: 0
SLAMon Agent Server Bypass: Disabled
SLAMon Agent Refuse Server Tests: Allow Tests
```

Next steps

If you have configured SLA Monitor yet the agent is not functioning as expected, perform typical troubleshooting steps to verify agent accessibility:

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

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

Variable definitions

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

Variable	Value
agent	Configures the SLA Monitor agent.
agent-comm-port *<0, 1024-65535>*	Configures the SLA Monitor agent-to-agent communication UDP port.
agent ip address *<A.B.C.D>*	Configures the agent IP address. If no IP address is specified, the default value is 0.0.0.0, which causes the agent to use the switch/stack IP address. **Note:** If you specify an IP address, ensure the address is a valid Layer 3 IPv4 address that is already configured for use by the switch.
agent port *<0, 1024-65535>*	Configures the UDP port for agent-server communication. The agent receives discovery packets on this port. The default is port 50011. The server must use the same port.
cli	Configures the SLA Monitor agent CLI interface.
cli-timeout *<60–600>*	Configures the CLI timeout value in seconds. The default is 60 seconds. **Note:** The CLI commands only impact the SLA Monitor CLI and not the standard platform CLI.
ntr	Initiates the SLA Monitor NTR test.
oper-mode	You can enable or disable the SLA Monitor agent. By default, SLA Monitor agent is disabled.

Table continues…

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

Executing NTR test using CLI

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

Before you begin

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

Procedure

1. Enter Application Configuration mode:

```
enable

configure terminal

application
```

2. Execute the NTR test:

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

Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#application
Switch(config-app)#slamon oper-mode enable
Switch(config-app)#slamon ntr 192.0.2.1 46

-------------------------------------------------
SLAMon Network Trace Report
-------------------------------------------------
Source IP/Port: 192.0.2.2:50013
Source DSCP Marking: 46
Destination IP/Port: 192.0.2.1:33434
Maximum TTL: 1
Request Result: OK (Port unreachable)
                  Ingress  Egress
IP Address         DSCP     DSCP      RTT (ms)
-------------------------------------------------
192.0.2.2           46        0       0.000
192.0.2.1           0         0       1.240
```

Variable definitions

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

Variable	Value
IPv4 Address *<A.B.C.D>*	Specifies the destination IP address. If no IP address is specified, the test execution fails.
DSCP *<0–63>*	Specifies the Differential Services Code Point (DSCP) value for use in packets that are generated by the NTR test.
attempts *<1–10>*	Specifies the number of attempts generated by the NTR test. The default value is 2.
period *<10000–200000>*	Specifies the interval between packets in microseconds, generated by the NTR test. The default interval is 20000 microseconds.

Executing RTP test using CLI

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

Before you begin

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

Note:

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

Procedure

1. Enter Application Configuration mode:

   ```
   enable

   configure terminal

   application
   ```

2. Execute the RPT test:

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

Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#application
Switch(config-app)#slamon oper-mode enable
Switch(config-app)#slamon rtp 192.0.2.1 46

-------------------------------------------------
SLAMon Real Time Protocol Network Report
-------------------------------------------------
Source IP/Port: 192.0.2.2:50012
Source DSCP Marking: 46
Destination IP/Port: 192.0.2.1:50012

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

Out-of-Order Arrivals:0

-------------------------------------------------
          Network Jitter - Quartiles (ms)
    0         1         2         3         4
-------------------------------------------------
    0.007     0.173     0.208     0.224     1.343
```

Variable definitions

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

Variable	Value
IPv4 Address *<A.B.C.D>*	Specifies the destination IP address. If no IP address is specified, the test execution fails.
DSCP *<0–63>*	Specifies the DSCP value for use in packets that are generated by the RTP test.

Table continues…

Variable	Value
npack <*10–100*>	Specifies the number of test packets generated by the RTP test. Test packets are used to determine jitter. The value ranges from 10 to 100. The default value is 50.
nsync <*10–100*>	Specifies the number of synchronization packets generated by the RTP test. Synchronization packets are used to determine network delay. The value ranges from 10 to 100. The default value is 10.
period <*10000–200000*>	Specifies the interval between packets in microseconds, generated by the RTP test. The default interval is 20000 microseconds.

Configuring SLA Monitor using EDM

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

Configuring SLA Monitor agent using EDM

Use this procedure to configure the SLA Monitor agent.

Procedure

1. In the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, click **SLA Monitor**.
3. In the **SLA Monitor** tab, enable the SLA Monitor agent and either accept the defaults or configure parameters as required.
4. On the toolbar, click **Apply**.

SLA Monitor tab field descriptions

Name	Description
Status	Enables or disables the SLA Monitor agent. The default is disabled. • **enabled**: enables the SLA Monitor agent • **disabled**: disables the SLA Monitor agent If you disable the agent, it does not respond to discover packets from a server.

Table continues…

Name	Description
	If you disable the agent because of resource concerns, consider changing the server configuration instead, to alter the test frequency or duration, or the number of targets.
ServerBypass	Enables or disables the SLA Monitor agent server bypass mode. • **enabled**: enables the SLA Monitor agent server bypass mode. • **disabled**: disables the SLA Monitor agent server bypass mode.
RefuseServerTests	Allows or refuses the NTR and RTP test requests from the server. • **allow**: the SLA Monitor agent server accepts test requests from the server with which it is registered. • **refuse**: the SLA Monitor agent rejects test requests from the server with which it is registered. Test requests originating from platform, SLM CLI interfaces, and SNMP are not affected.
ConfiguredAgentToAgentPort	Specifies the UDP port utilized by the SLA Monitor agent for agent-agent communication. If the value of this attribute is zero, the SLA Monitor agent utilizes a default port value for the base agent-agent UDP communication port.
ConfiguredAgentAddrType	Indicates IPv4–based communications.
ConfiguredAgentAddr	Specifies the agent IP address. The default value is 0.0.0.0, which causes the agent to use the switch/stack IP address.
ConfiguredAgentPort	Specifies the UDP port for agent-server communication. The agent receives discovery packets on this port. The default is port 50011. The server must use the same port.
CliAvailable	Specifies whether SLA Monitor agent CLI is available or not available.
CliTimeout	Configures the CLI timeout value in seconds. The default is 60 seconds.
CliTimeoutMode	Specifies the maximum amount of time, in seconds, until the CLI session is automatically terminated. The value of this attribute is pertinent only if CLI time-outs are enabled. The default is 60 seconds.
ConfiguredServerAddrType	Indicates IPv4–based communications.

Table continues…

Name	Description
ConfiguredServerAddr	Specifies the server IP address. If an IP address is specified, the agent is restricted to use this server IP address. The default is 0.0.0.0, which allows the agent to register with any server.
ConfiguredServerPort	Specifies the server port. The default is 0, which allows the agent to disregard the source port information in server traffic. The server must use the same port.
ConfiguredAltServerAddrType	Indicates IPv4–based communications.
ConfiguredAltServerAddr	Specifies a secondary server IP address.
SupportApps	Indicates SLA Monitor supported applications. This is a read-only field.
AgentAddressType	Indicates IPv4–based communications. This is a read-only field.
AgentAddress	Indicates the agent IP address. This is a read-only field.
AgentPort	Indicates the agent port. This is a read-only field.
RegisteredWithServer	Indicates whether the agent is registered with a server. This is a read-only field.
RegisteredServerAddrType	Indicates IPv4–based communications. This is a read-only field.
RegisteredServerAddr	Indicates IP address of the Avaya Diagnostic Server with which the agent is registered. This is a read-only field.
RegisteredServerPort	Indicates the TCP port used by the Avaya Diagnostic Server with which the agent is registered. This is a read-only field.
RegistrationTime	Indicates the time in seconds, since the agent registered with the server. This is a read-only field.
AgentToAgentPort	Indicates the base UDP port used by the SLA Monitor agent for agent-to-agent communication. The base UDP port is used to derive multiple agent communication ports. This is a read-only field.
EncryptionSupport	Indicates if encrypted agent-server communication is supported.

Executing a new trace route (NTR) test using EDM

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

Important:

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

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **SLA Monitor**.
3. In the SLA Monitor work area, click **NTR**.
4. In the NTR work area, click **Insert** to enter parameters for the new test.
5. In the **OwnerId** dialog box, type the owner id.
6. In the **TestName** dialog box, type the test name.
7. In the **TargetAddress** dialog box, type the target IP address.
8. In the **Dscp** dialog box, type the dscp value (0-63).
9. In the **Attempts** dialog box, type the number of attempts (1-10).
10. In the **Period** dialog box, type the type the duration in microseconds (1000–200000).
11. In the **Label** dialog box, type the label.
12. Click **enabled** to enable the administrator status.
13. Click **Insert** to initiate the NTR test.
14. In the NTR work area, click **Results** to view the test results.

NTR field descriptions

Name	Description
OwnerId	Specifies the owner of an NTR test.
TestName	Specifies the name of an NTR test.
TargetAddress	Specifies the target IP address for the NTR test.
Dscp	Specifies the Differential Services Code Point (DSCP) value for use in packets that are generated by the NTR test.
Attempts	Specifies the number of attempts generated by the NTR test. The default value is 2.
Period	Specifies the interval between packets in microseconds, generated by the NTR test. The default interval is 20000 microseconds.
Label	Specifies the text label used to reference the NTR control entry.
AdminStatus	Specifies the administrator status. You must enable the administrator status to initiate the NTR test. The administrator status is disabled by default.

Viewing new trace route test results

Use this procedure to view the new trace route (NTR) test results.

Before you begin

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

Procedure

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

NTR Results tab field descriptions

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

Executing a real time protocol (RTP) test using EDM

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

Important:

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

Note:

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

Procedure steps

1. From the navigation tree, double-click **Serviceability**.
2. In the Serviceability tree, double-click **SLA Monitor**.
3. In the SLA Monitor work area, click **RTP**.
4. In the RTP work area, click **Insert** to enter parameters for the new test.
5. In the **OwnerId** dialog box, type the owner id.
6. In the **TestName** dialog box, enter the test name.
7. In the **TargetAddress** dialog box, type the target IP address.
8. In the **Dscp** dialog box, type the dscp value (0–63).
9. In the **TestPackets** dialog box, type the number of test packets (10–100).
10. In the **SyncPackets** dialog box, type the number of synchronization packets (10–100).
11. In the **Period** dialog box, type the type the duration in microseconds (1000–200000).
12. Click **enabled** to enable the administrator status.
13. In the **Label** dialog box, type the label.
14. Click **Insert** to initiate the RTP test.
15. In the RTP work area, click **Results** to view the test results.

RTP field descriptions

Name	Description
OwnerId	Specifies the owner of an RTP test.
TestName	Specifies the name of an RTP test.
TargetAddress	Specifies the target IP address for the RTP test.
Dscp	Specifies the Differential Services Code Point (DSCP) value for use in packets that are generated by the RTP test.
TestPackets	Specifies the number of test packets generated by the RTP test. Test packets are used to determine jitter.
SyncPackets	Specifies the number of synchronization packets generated by the RTP test. Synchronization packets are used to determine network delay.
Period	Specifies the interval between packets in microseconds, generated by the RTP test. The default interval is 20000 microseconds.

Table continues…

Name	Description
Label	Specifies the text label used to reference the RTP control entry.
AdminStatus	Specifies the administrator status. You must enable the administrator status to initiate the RTP test. The administrator status is disabled by default.

Viewing real time protocol test results

Use this procedure to view the real time protocol (RTP) test results.

Before you begin

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

Procedure

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

RTP Results tab field descriptions

Name	Description
OperStatus	Indicates the status of an RTP test. • **inProgess** indicates that an RTP test is in progress. • **aborted** indicates that an RTP test is aborted. • **completed** indicates that an RTP test is completed.
SrcAddress	Indicates the source IP address used for the RTP test.
SrcPort	Indicates the port used for the RTP test.
DstAddress	Indicates the destination IP address used for the RTP test.
DstPort	Indicates the destination port used for the RTP test.
Dscp	Specifies the Differential Services Code Point (DSCP) value for use in packets that are generated by the RTP test.

Table continues…

Name	Description
AverageDelay	Indicates the average network delay (RTT) experienced during the RTP test execution in microseconds.
MedianDelay	Indicates the median network delay experienced during an RTP test execution in microseconds.
PacketLoss	Indicates the count of packets lost during an RTP test execution.
OutOfOrderArrivals	Indicates the count of packets arriving out-of-order during an RTP test execution.
JitterQuartile0 – JitterQuartile5	Indicates the resulting quartile boundaries after sorting the network jitter values of all test packets during an RTP test execution. The value is represented in microseconds
AbortData	Indicates the details of the RTP test that was aborted.