Nortel Ethernet Routing Switch 4500 Series

Configuration — System Monitoring

Release: 5.3
Document Revision: 05.01

www.nortel.com

NN47205-502

Nortel Ethernet Routing Switch 4500 Series
Release: 5.3
Publication: NN47205-502
Document release date: 27 April 2009

Sourced in Canada

Contents

Software licence

This section contains the Nortel Networks software license.

Nortel Networks Inc. software license agreement

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms

of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General 1. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights

to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

2. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

3. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

4. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

5. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

6. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

New in this release

The following sections detail what's new in *Nortel Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502) for Release 5.3.

- "Features" (page 11)

Features

See the following sections for information about feature changes:

- "Trap Web page" (page 11)
- "Management Information Base Web page" (page 11)
- "Show Environmental" (page 12)

Trap Web page

Trap Web page offers a graphical method to enable or disable the traps you want to send. In the case of multiple trap receivers, you can use Web-based management the WebUI to map the traps that each receiver receives. See

- "Trap Web page" (page 17)
- "Using the trap Web page to control the generation of traps" (page 67)

Management Information Base Web page

The MIB Web Page offers a Web interface from which you can access SNMP MIBs. From the Web interface, you can access the MIB objects of a switch either by object name or by OID , and do simple SNMP requests on them. See

- "MIB Web page" (page 17)
- "Using the MIB Web page for SNMP Get and Get-Next" (page 66)
- "Using the MIB Web page for SNMP walk" (page 66)

Show Environmental

The Show Environmental feature provides the environmental information on the working of the switch or stack. The information is available through NNCLI commands, Device Manager and SNMP. See

- “Show Environmental” (page 28)
- “Viewing Environmental status using NNCLI” (page 80)
- “Display of Environmental status using Device Manager” (page 83)

Introduction

This document provides information you need to configure and use system monitoring for the Ethernet Routing Switch 4500 series Release 5.3.

Navigation

System monitoring fundamentals

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

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

CPU and memory utilization

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

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

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

Light Emitting Diode (LED) on the Nortel Ethernet Routing Switch 4500 Series

The Ethernet Routing Switch 4500 Series displays diagnostic and operation information through the LEDs on the unit. Familiarize yourself with the interpretation of the LEDs on the 4500 series device. For detailed information regarding the interpretation of the LEDs, see*Nortel Ethernet Routing Switch 4500 Series — Installation* (NN47205-300).

Remote logging

The remote logging feature that originates in Software Release 5.1 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.

Configuring remote logging with Device Manager

Configure remote logging with Device Manager (DM) to provide functionality for managing remote logging.

Step	Action
1	Open the **System Log** window by choosing **Edit, Diagnostics, System Log** from the menu. Select the **Remote System Log** tab.
2	In the fields provided, enter the remote logging information. The following table describes Remote System Log tab fields.

Table 1
Remote System Log tab fields

Field	Description
Address	The IP address of the remote syslog server.
Enabled	Enables or disables remote logging.
SaveTargets	Sets the severity level of messages that are saved to the remote server.
RemoteSyslogAddressType	The type of address for the remote system log.
RemoteSyslogAddress	Address of the remote system log.

3	Click **Apply**.

--End--

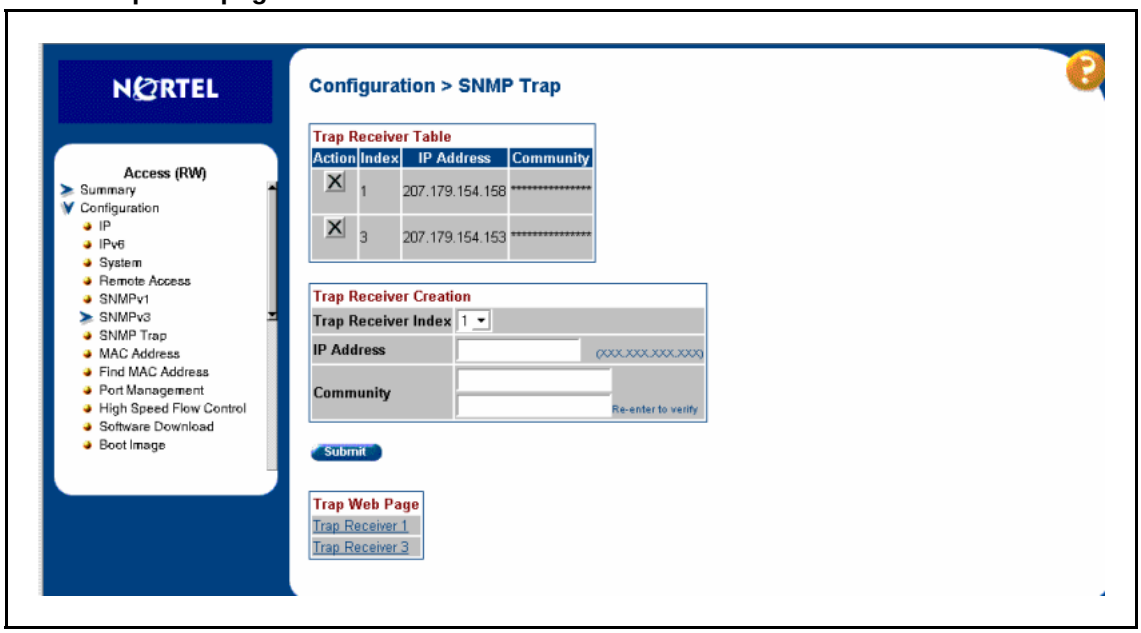
Trap Web page

Trap Web page provides a graphical method to enable or disable traps you want to send. In the case of multiple trap receivers, you can specify which traps go to which receiver. The selection of traps that a certain receiver gets depends on criteria like security, network connectivity, or other information that is important to that particular receiver.

You can access a separate Trap Web page for every host, from which you can enable or disable any of the listed traps. You can access those pages through the SNMP Trap Web page, which contains two options for every trap. The first option enables the trap. The second option disables the trap. Select an option to enable or disable a specific trap for a specific host. You can identify the traps by their associated System Log entry (a message is logged in the System Log whenever a trap is issued).

For more information about the Traps for DHCP Snooping, Dynamic ARP Inspection (DAI), and IP Source Guard (IPSG), see *Nortel Ethernet Routing Switch 4500 Series Configuration-Security* (NN47205-505).

Figure 1
SNMP Trap Web page



MIB Web page

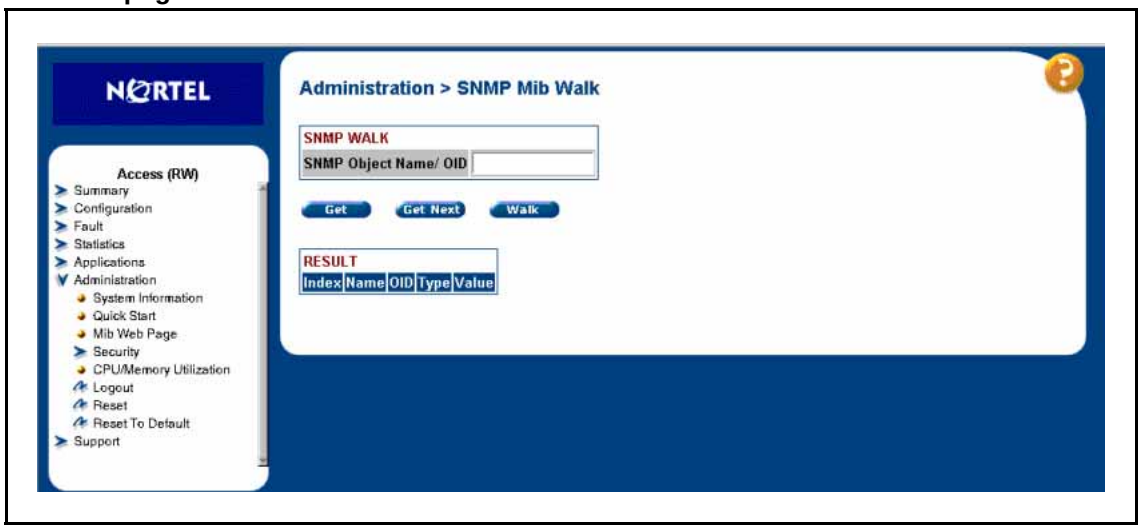
With Web-based management, you can see the response of an SNMP Get and Get-Next request for an Object Identifier (OID) or object name.

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

The MIB Web page does not support the following features:

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

Figure 2
Mib Web page



IGMP and the system event log

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

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

- critical
- serious
- informational

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

- IGMP initialization
- configuration changes

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

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

In the table Table 2 " IGMP syslog messages" (page 19):

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

Table 2 " IGMP syslog messages" (page 19) describes the IGMP syslog messages and their severity.

Table 2
IGMP syslog messages

Severity	Log Messages
Informational	IGMP initialization success
Critical	IGMP initialization failed: Error code %d
Informational	IGMP policy initialized
Informational	IGMP configuration loaded successfully
Informational	IGMP configuration failed: Loaded to factory default
Informational	IGMP configuration changed: Snooping enabled on VLAN %d
Informational	IGMP configuration changed: Snooping disabled on VLAN %d
Informational	IGMP configuration changed: Proxy enabled on VLAN %d
Informational	IGMP configuration changed: Proxy disabled on VLAN %d
Informational	IGMP configuration changed: Query time set to %d on VLAN %d
Informational	IGMP configuration changed: Robust value set to %d on VLAN %d
Informational	IGMP configuration changed: Version %d router port mask 0x%x set on VLAN %d
Informational	IGMP configuration changed: Unknown multicast filter enabled
Informational	IGMP configuration changed: Unknown multicast filter enabled
Informational	IGMP configuration changed: Trunk %d created for IGMP

Table 2
IGMP syslog messages (cont'd.)

Severity	Log Messages
Informational	IGMP configuration changed: Trunk %d removed for IGMP ports
Informational	IGMP configuration changed: Mirror ports set
Informational	IGMP configuration changed: Port %d added to VLAN %d
Informational	IGMP configuration changed: Port %d removed from VLAN %d
Informational	IGMP new Querier IP %x learned on port %d
Informational	IGMP exchange database sent by unit %d
Informational	IGMP exchange database received on unit %d from %d
Informational	IGMP exchange database done
Informational	IGMP stack join completed
Serious	IGMP not able to join stack: Error code %d
Informational	IGMP exchange group database sent by unit %d
Informational	IGMP exchange group database received on unit %d from %d
Informational	IGMP received report on VLAN %d for Group 0x%x on port %d
Informational	IGMP received leave on VLAN %d for Group 0x%x on port %d
Informational	IGMP received query on VLAN %d for Group 0x%x on port %d
Informational	IGMP dynamic router port %d added
Informational	IGMP dynamic router port %d removed

Stack Monitor

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

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

With the Stack Monitor feature, when a stack is broken, the stack and any disconnected units from the stack, send Simple Network Management Protocol (SNMP) traps. If the stack or the disconnected units are still connected to the network, they generate log events and send trap messages to the management station to notify the administrator of the

event. After the problem is detected, the stack and disconnected units continue to generate log events and send traps at a user-configurable interval until the situation is remedied (or the feature is disabled).

Local ports shutdown while stacking

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

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

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

Stack loopback test

The stack loopback test feature allows the customer to quickly test the switch stack ports and the stack cables on 4500 units. This feature helps you while experiencing stack problems to determine whether the root cause is a bad stack cable or a damaged stack port and prevents potentially good switches being returned for service. You can achieve this by using two types of loopback tests:

- “Internal loopback test” (page 21)
- “External loopback test” (page 22)

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

Internal loopback test

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

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

External loopback test

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

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

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

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

ATTENTION

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

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

Port mirroring

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

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

ATTENTION

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

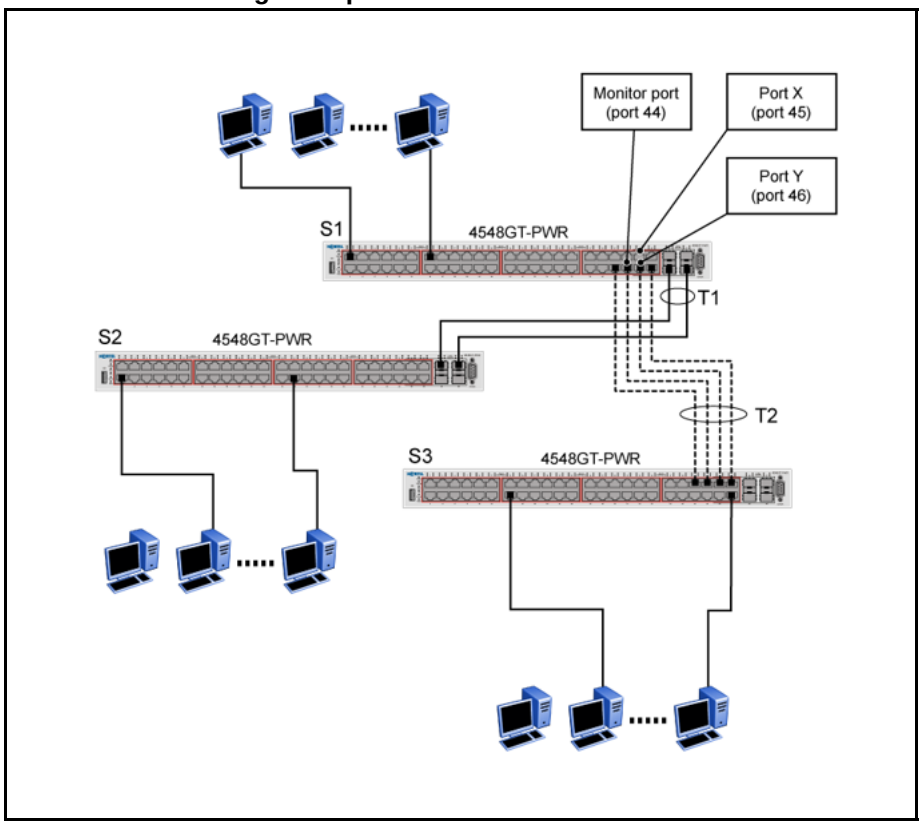
ATTENTION

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

Port-based mirroring configuration

The figure Figure 3 "Port-based mirroring example" (page 23) shows an example of a port-based mirroring configuration in which port 20 is designated as the monitor port for ports 21 and 22 of Switch S1. Although this example shows ports 21 and 22 monitored by the monitor port (port 20), you can monitor any of the trunk members of T1 and T2.

Figure 3
Port-based mirroring example



This example shows port X and port Y as members of Trunk T1 and Trunk T2. Port X and port Y are not required to always be members of Trunk T1 and Trunk T2.

ATTENTION
You cannot configure trunk members as monitor port.

In the configuration example shown in, you can set the designated monitor port (port 44) to monitor traffic in any of the following modes:

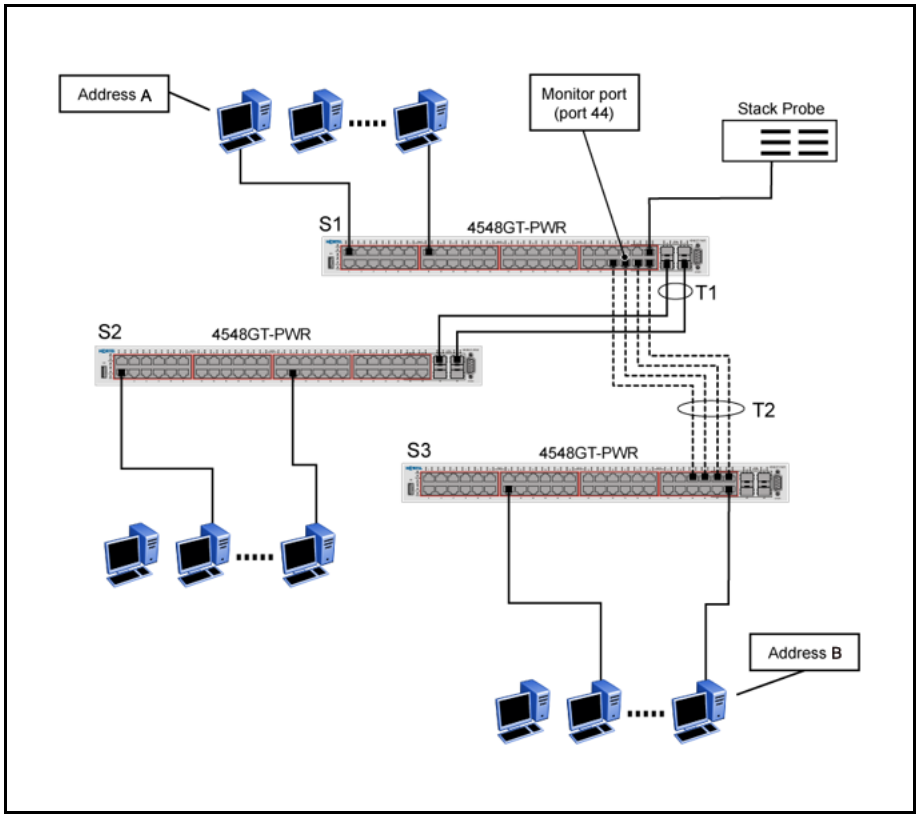
- Monitor all traffic received by port X.
- Monitor all traffic transmitted by port X.
- Monitor all traffic received and transmitted by port X.
- Monitor all traffic received by port X or transmitted by port Y.

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

Address-based mirroring configuration

The figure Figure 4 "Address-based mirroring example" (page 24) shows an example of an address-based mirroring configuration in which port 20, the designated monitor port for Switch S1, monitors traffic occurring between address A and address B.

Figure 4
Address-based mirroring example



In this configuration, you can set the designated monitor port (port 44) to monitor traffic in any of the following modes:

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

Remote Network Monitoring (RMON)

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

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

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

RMON has the three following major functions:

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

RMON scaling

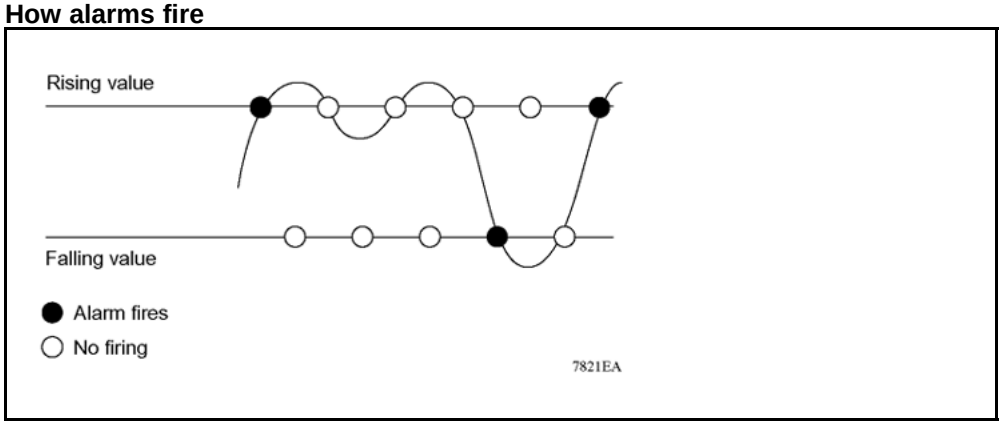
The number of RMON alarm instances per stack has increased from 400 to 800 with release 5.2 for the Ethernet Routing Switch 4500 series products.

Working of RMON alarms

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

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

Figure 5
How alarms fire



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

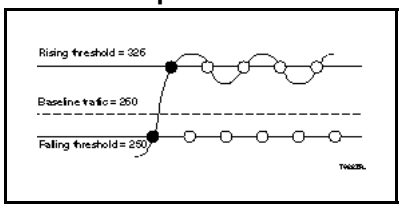
A general guideline is to define one of the threshold values to an expected baseline value, and then define the opposite threshold as the out-of-bounds limit. Because of sample averaging, the value may be equal to ±1 of the baseline units. For example, assume an alarm is defined on octets going out of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

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

You define the alarm with a falling threshold less than 260 (assuming the alarm polling interval is 10 seconds), say 250, the rising alarm can fire only once (see the following figure Figure 6 "Alarm example - threshold less than 260" (page 27)). 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 would cause the value for outbound octets to drop to zero), the falling alarm cannot fire because the

baseline traffic is always greater than the value of the falling threshold. By definition, the failure of the falling alarm to fire prevents the rising alarm from firing a second time.

Figure 6
Alarm example - threshold less than 260



Creating alarms

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

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

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

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

RMON events and alarms

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

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

- Rising Event
- Falling Event

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

How events work

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

- RisingEvent
- FallingEvent

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

Show Environmental

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

- power supply status
- fan status
- switch system temperature

The Show Environmental command depends on the hardware of each unit. The command is available from any NNCLI mode, and you do not need to enable or activate this feature. The command displays information for a stand-alone switch and for each unit in a stack, regardless of how many units are in that stack.

You can configure the Show Environmental command in NNCLI, SNMP, Device Manager and Web based management.

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

Table 3
Environmental parameters

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

Network monitoring configuration using NNCLI

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

Navigation

Configuring system log using the NNCLI

This section describes the NNCLI commands that you use to configure and manage the system log.

Viewing CPU utilization using NNCLI

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

Procedure steps

Step	Action
1	Enter Privileged exec mode to access the commands required.

2 Enter the **show cpu-utilization** command.

3 Observe the displayed information.

--End--

Job Aid

The following figure is an example of CPU utilization output.

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

        CPU Utilization
--------------------------------------------------------------------

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

Viewing memory utilization using NNCLI

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

Procedure steps

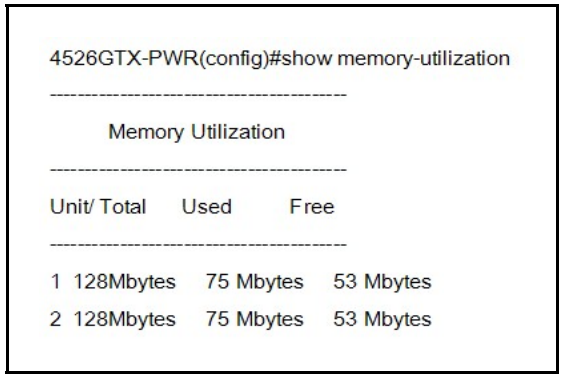
Step	Action
1	Enter Privileged exec mode to access the commands required.
2	Enter the **show memory-utilization** command.
3	Observe the displayed information.

--End--

Job Aid

The following figure is an example of memory utilization output.

Figure 7
Example memory utilization output



Viewing system logging

View logging using the NNCLI.

Procedure steps

Step	Action
1	Enter Privileged exec mode.
2	Enter the **`show logging`** command.
3	Observe the displayed information.

--End--

Run the **`show logging`** command in Privileged EXEC command mode.

Variable definitions

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

Configuring syslog capabilities

Use this procedure to display and clear the last software exception

Procedure Steps

Step	Action
1	Use the **enable** command to enter Priv Exec mode.
2	Enter the **show system last-exception [unit { <1-8> | all }]** command to show the last software exception
3	Enter the **clear last-exception [unit { <1-8> | all }]** command to clear the last software exception

--End--

Variable definitions

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

Job Aid

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

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

bld version: 1.0.25.0 time: (25/Jan/07 18:29:25) view: (icamana_b)
sysUpTime: 104511 Registers:

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

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

Configuring logging using NNCLI

Configure logging using the NNCLI to configure the system settings for the system event log.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **logging [enable | disable] [level critical | serious | informational | none] [nv-level critical**

| **serious** | **none] remote [address** | **enable** | **level] volatile [latch** | **overwrite]** command.

--End--

Variable definitions

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

Disabling logging using NNCLI

Disables the system event log.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **no logging** command.

--End--

Default logging using NNCLI

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

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **default logging** command.

--End--

Clearing log messages

The **clear logging** command clears all log messages in DRAM.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **clear logging [non-volatile] [nv] [volatile]** command.

--End--

Variable Definitions

The following table describes the command parameters.

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

Network monitoring configuration using Device Manager

This chapter describes the procedures you can use to configure network monitoring using Device Manager

Navigation

Viewing CPU and memory utilization

Use this procedure to view both CPU and memory utilization.

Step	Action
1	Navigate to **Edit, Chassis**
2	Select the **CPU/Mem Utilization** tab
3	Click the **Refresh** button to update the data.

--End--

Job Aid

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

Field	Description
Unit	The numerical representation of the unit.

Field	Description
Last10Seconds	CPU usage, in percentage, for the last 10 seconds.
Last1Minute	CPU usage, in percentage, for the last minute.
Last10Minutes	CPU usage, in percentage, for the last 10 minutes.
Last1Hour	CPU usage, in percentage, for the last hour.
Last24Hours	CPU usage, in percentage, for the last 24 hours.
TotalCPUUsage	CPU usage in percentage, since system start up.
MemoryTotalMB	Total memory present, in megabytes, on the unit.
MemoryAvailableMB	Memory remaining available on the unit.

Configuring the system log with Device Manager

Use Device Manager (DM) to manage the system log. To configure the system log, perform the following procedure.

Procedure Steps

Step	Action
1	Open the **System Log** window by selecting **Edit, Diagnostics, System Log** from the menu.
2	Select the **System Log Settings** tab.
3	In the fields provided, configure the system log settings. The following table describes the system log settings fields.
4	Click **Apply**.

--End--

Job Aid

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

Field	Description
Operation	Turns the system log on or off.
BufferFullAction	Specifies whether the system log overwrites itself or discontinues the storage of messages when the buffer is full.
Volatile - CurSize	Shows the current number of messages stored in volatile memory.

Field	Description
Volatile - SaveTargets	Selects the severity of system messages to save.
non-Volatile - CurSize	Shows the current number of messages stored in non-volatile memory.
non-Volatile - SaveTargets	Selects the severity of system messages to save.
ClearMessageBuffers	Selects the sections of the system log to delete.

Creating a graph using Device Manager

Use Device Manager (DM) to view and make use of statistical information gathered by the switch. You can convert this statistical information to a bar, line, area, or pie graph.

Procedure steps

Step	Action
1	After opening a window that provides graphing capabilities and selecting the desired tab, select the information to graph do one of the following: • Click and drag the mouse across the rows and columns of data to graph. • Hold the **Control (CTRL)** key and click on the cells of data to graph. • Hold the **Shift** key and click a range of data to graph.
2	Press the graph button that corresponds to the type of graph.

--End--

Job Aid

The following figure depicts the graph buttons.

Graphing switch chassis data

This section describes how you can use Device Manager (DM) to view switch chassis statistical information in a variety of graphs.

Navigation

- “Viewing the SNMP tab” (page 40)
- “Viewing the IP tab” (page 42)

Viewing the SNMP tab

View the SNMP tab to view the read-only information about SNMP activity on the switch.

Procedure Steps

Step	Action
1	Open the **Graph Chassis** window by selecting **Graph, Chassis** from the menu. The **Graph Chassis** window opens.
2	Select the **SNMP** tab if it is not selected.

--End--

Job Aid

The following table describes the fields on this tab.

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

InGetResponses	The total number of SNMP Get-Response PDUs accepted and processed by the SNMP protocol.
OutTraps	The total number of SNMP Trap PDUs generated by the SNMP protocol.
OutTooBigs	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is tooBig.
OutNoSuchNames	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is noSuchName.
OutBadValues	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is badValue.
OutGenErrs	The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is genErr.
InBadVersions	The total number of SNMP messages delivered to the SNMP protocol for an unsupported SNMP version.
InBadCommunityNames	The total number of SNMP messages delivered to the SNMP protocol that used an unknown SNMP community name.
InBadCommunityUses	The total number of SNMP messages delivered to the SNMP protocol that represented an SNMP operation not allowed by the SNMP community named in the message.
InASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP protocol when decoding received SNMP messages.
InTooBigs	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is tooBig.
InNoSuchNames	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is noSuchName.
InBadValues	The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is badValue.

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

Viewing the IP tab

View the IP tab to view the read-only information about IP activity on the switch.

Procedure Steps

Step	Action
1	Open the **Graph Chassis** window by selecting **Graph, Chassis** from the menu. The Graph Chassis window opens.
2	Select the **IP** tab.

--End--

Job Aid

The following table describes the fields on this tab.

Table 4
IP tab fields

Field	Description
InReceives	The total number of input datagrams received from interfaces, including those received in error.
InHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, and errors discovered in processing the datagram IP options.
InAddrErrors	The number of input datagrams discarded because the IP address in the IP header destination field is 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 is not a local address.

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

Viewing the ICMP In tab

View the ICMP In tab to view the read-only information about ICMP In activity on the switch.

Procedure Steps

Step	Action
1	Open the **Graph Chassis** window by selecting **Graph, Chassis** from the menu. The Graph Chassis window opens.
2	Select the **ICMP In** tab.

--End--

Job aid

The following table describes the ICMP In tab.

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

Viewing the ICMP Out tab

View the ICMP Out tab to view the read-only information about ICMP Out activity on the switch.

Procedure Steps

Step	Action
1	Open the **Graph Chassis** window by selecting **Graph, Chassis** from the menu. . The Graph Chassis window opens

2 Select the **ICMP Out** tab.

--End--

Job Aid

The following table describes the ICMP Out tab.

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

Viewing the TCP tab

View the TCP tab to view the read-only information about TCP activity on the switch.

Procedure Steps

Step	Action
1	Open the **Graph Chassis** window by selecting **Graph, Chassis** from the menu. The Graph Chassis window opens.
2	Select the **TCP** tab.

--End--

Job Aid

The following table describes the fields on the TCP tab.

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

Viewing the UDP tab

View the UDP tab to view the read-only information about UDP activity on the switch.

Procedure Steps

Step	Action
1	Open the **Graph Chassis** window by selecting **Graph, Chassis** from the menu. The Graph Chassis window opens.

2 Select the **UDP** tab.

--End--

Job Aid

The following table describes the fields on the UDP tab.

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

Graphing switch port data

This section describes how you can use Device Manager (DM) to view switch port statistical information in a variety of graphs.

Navigation

- "Viewing the Interface tab" (page 47)
- "Viewing the Ethernet Errors tab" (page 49)
- "Viewing the Bridge tab" (page 52)
- "Viewing the RMON tab" (page 53)
- "Viewing the EAPOL Stats tab" (page 54)
- "Viewing the EAPOL Diag tab" (page 55)
- "Viewing the LACP tab" (page 58)
- "Viewing the Misc tab" (page 59)

Viewing the Interface tab

View the Interface tab to view the read-only information about the selected interfaces.

Procedure Steps

Step	Action
1	Open the **Graph Port** window by selecting one or multiple ports on the **Device View**, and then choose **Graph, Port** from the menu.
2	Select the **Interface** tab.

--End--

Job Aid

The following table describes the fields on the Interface tab

Field	Description
InOctets	The total number of octets received on the interface, including framing characters.
OutOctets	The total number of octets transmitted out of the interface, including framing characters.
InUcastPkts	The number of packets delivered by this sublayer to a higher sublayer that are not addressed to a multicast or broadcast address at this sublayer.
OutUcastPkts	The number of packets that higher-level protocols requested to be transmitted that are not addressed to a multicast address at this sublayer. This total number includes those packets discarded or unsent.
InDiscards	The number of inbound packets that are chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
OutDiscards	The number of outbound packets which are chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
InErrors	For packet-oriented interfaces, the number of inbound packets that contain errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contain 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.

Field	Description
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 0.
InMulticastPkts	The number of packets delivered by this sublayer to a higher sublayer that are addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both group and functional addresses.
OutMulticasttPkts	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 are discarded or not sent. For a MAC layer protocol, this number includes both group and functional addresses.
InBroadcastPkts	The number of packets delivered by this sublayer to a higher sublayer that are addressed to a broadcast address at this sublayer.
OutBroadcastPkts	The number of packets that higher-level protocols requested be transmitted, and that are addressed to a broadcast address at this sublayer, including those that are discarded or not sent.

Viewing the Ethernet Errors tab

View the Ethernet Errors tab to view read-only information about port Ethernet error statistics.

Procedure Steps

Step	Action
1	Open the **Graph Port** window by selecting one or multiple ports on the **Device View** and then selecting **Graph, Port** from the menu. The **Graph Port** window opens.
2	Select the **Ethernet Errors** tab.

--End--

Job Aid

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

Field	Description
AlignmentErrors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
FCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
InternalMacTransmitErrors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object.
InternalMacReceiveErrors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object. The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object can represent a count of receive errors on a particular interface that are not otherwise counted.

Field	Description
CarrierSenseErrors	The number of times that the carrier sense condition is lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once for each transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.
FrameTooLongs	A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
SQETestErrors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985, and its generation is described in section 7.2.4.6 of the same document.
DeferredTransmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object.
MultipleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.

Field	Description
LateCollisions	The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
ExcessiveCollisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.

Viewing the Bridge tab

View the Bridge tab to view the read-only information about port frame statistics.

Procedure Steps

Step	Action
1	Open the **Graph Port** window by selecting one or multiple ports on the **Device View**, and then choose **Graph, Port** from the menu. The **Graph Port** window opens.
2	Select the **Bridge** tab.

--End--

Job Aid

The following table describes the fields on the Bridge tab.

Field	Description
DelayExceededDiscards	Number of frames discarded by the port due to excessive transit delays through the bridge. It is incremented by both transparent and source route bridges.
MtuExceededDiscards	Number of frames discarded by the port due to an excessive size. It is incremented by both transparent and source route bridges.
InFrames	The number of in frames received by this port from its segment.
OutFrames	The number of out frames received by this port from its segment.
InDiscards	Count of valid frames received which are discarded (filtered) by the Forwarding Process.

Viewing the RMON tab

View the RMON tab to view read-only remote monitoring statistics.

Procedure Steps

Step	Action
1	Open the **Graph Port** window by selecting one or multiple ports on the **Device View**, and then choosing **Graph, Port** from the menu. The **Graph Port** window opens.
2	Select the **RMON** tab.

--End--

Job Aid

The following table describes the fields on the RMON tab.

Field	Description
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
BroadcastPkts	The total number of good packets received that are directed to the broadcast address. This does not include multicast packets.
MulticastPkts	The total number of good packets received that are directed to a multicast address. This number does not include packets directed to the broadcast address.
CRCAlignErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
UndersizePkts	The total number of packets received that are less than 64 octets long (excluding framing bits but including FCS octets) and are otherwise well formed.
OversizePkts(>1518)	The total number of packets received that are longer than 1518 octets (excluding framing bits but including FCS octets) and are otherwise well formed.

Field	Description
Fragments	The total number of packets received that are less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). It is entirely normal for etherStatsFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Jabbers	The total number of packets received that are longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
1..64	The total number of packets (including bad packets) received and transmitted that are between 1 and 64 octets in length (excluding framing bits but including FCS octets).
65..127	The total number of packets (including bad packets) received and transmitted that are between 65 and 127 octets in length (excluding framing bits but including FCS octets).
128..255	The total number of packets (including bad packets) received and transmitted that are between 128 and 255 octets in length (excluding framing bits but including FCS octets).
256..511	The total number of packets (including bad packets) received and transmitted that are between 256 and 511 octets in length (excluding framing bits but including FCS octets).
511..1023	The total number of packets (including bad packets) received and transmitted that are between 511 and 1023 octets in length (excluding framing bits but including FCS octets).
1024..1518	The total number of packets (including bad packets) received and transmitted that are between 1024 and 1518 octets in length (excluding framing bits but including FCS octets).

Viewing the EAPOL Stats tab

View the Extensible Authentication Protocol over LAN (EAPOL) Stats tab to view the read-only EAPOL statistics.

Procedure Steps

Step	Action
1	Open the **Graph Port** window by selecting one or multiple ports on the **Device View**, and then choosing **Graph, Port** from the

menu.
The **Graph Port** window opens.

2 Select the **EAPOL Stats** tab.

--End--

Job Aid

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

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

Viewing the EAPOL Diag tab

View the EAPOL Diag tab to view the read-only EAPOL diagnostic statistics.

Procedure Steps

Step	Action
1	Open the **Graph Port** window by selecting one or multiple ports on the **Device View**, and then choosing **Graph, Port** from the menu. The **Graph Port** window opens.

2 Select the **EAPOL Diag** tab.

--End--

Job Aid

The following table describes the fields on the EAPOL Diag tab.

Field	Description
EntersConnecting	Counts the number of times that the Authenticator Physical Address Extention (PAE) state the switch transitions to the Connecting state from any other state.
EapLogoffsWhileConnecting	Counts the number of times that the Authenticator PAE state machine transitions from Connected to Disconnected as a result of receiving an EAPOL-Logoff message.
EntersAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Connecting to Authenticating as a result of receiving an EAP-Response/Identity message from the supplicant.
AuthSuccessWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Authenticated as a result of the Backend authentication state machine indicating successful authentication of the supplicant.
AuthTimeoutsWhile Authenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of the Backend authentication state machine indicating authentication timeout.
AuthFailWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Held as a result of the Backend authentication state machine indicating authentication failure.
AuthReauthsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of a reauthentication request.

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

Field	Description
BackendAuthSuccesses	Counts the number of times that the Backend Authentication state machine receives an EAP-success message from the Authentication server.
BackendAuthFails	Counts the number of times that the Backend Authentication state machine receives an EAP-failure message from the Authentication server.

Viewing the LACP tab

View the LACP tab to view read-only Link Aggregation Control Protocol (LACP) diagnostic statistics.

Procedure Steps

Step	Action
1	Open the **Graph Port** window by selecting one or multiple ports on the **Device View**, and then choosing**Graph, Port** from the menu. The **Graph Port** window opens.
2	Select the **LACP** tab.

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

--End--

Job Aid

The following table describes the fields on the LACP tab.

Table 5
Field Descriptions

Field	Description
LACPDUsRX	Denotes the number of valid LACPDUs received on this Aggregation Port. This value is read-only.
MarkerPDUsRX	Signifies the number of valid Marker PDUs received on this Aggregation Port. This value is read-only.
MarkerResponsePDUsRX	The number of valid Marker Response PDUs received on this Aggregation Port. This value is read-only.

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

Viewing the Misc tab

View the Misc tab to display statistical information that does not belong grouped with the other tabs.

Procedure Steps

Step	Action
1	Open the **Graph Port** window by selecting one or multiple ports on the **Device View**, and then choosing **Graph, Port** from the menu. The **Graph Port** window opens.
2	Select the **Misc** tab.

--End--

Job Aid

The following table outlines the fields in the Misc tab.

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

Graphing Multi-Link Trunking (MLT) statistics

This section describes how you can use Device Manager (DM) to view (MLT) statistical information in a variety of graphs.

Navigation

- "Viewing the Interface tab" (page 60)
- "Viewing the Ethernet Errors tab" (page 61)

Viewing the Interface tab

View the Interface tab to view read-only statistical information about the selected Multilink Trunk.

Procedure Steps

Step	Action
1	Open the **MLT_LACP** window by selecting **VLAN, MLT/LACP** from the menu. This window opens with the **VLACP Global** tab selected.
2	Click on **Multilink Trunks** tab.
3	On the Multilink Trunks tab, select the row that represents the MLT to graph and then click the **Graph** button. The **MLT Statistics** window opens with the **Interface** tab selected.

--End--

Job Aid

The following table describes the fields on the Interface tab.

Field	Description
InMulticastPkt	The number of packets delivered to this MLT that are addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.
OutMulticast	The total number of packets that higher-level protocols requested to be transmitted, and that are addressed to a multicast address at this MLT, including those that are discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
InBroadcastPkt	The number of packets delivered to this MLT that are addressed to a broadcast address at this sublayer.

Field	Description
OutBroadcast	The total number of packets that higher-level protocols requested to be transmitted, and that are addressed to a broadcast address at this MLT, including those that are discarded or not sent.
HCInOctets	The total number of octets received on the MLT interface, including framing characters.
HCOutOctets	The total number of octets transmitted out of the MLT interface, including framing characters.
HCInUcastPkts	The number of packets delivered by this MLT to higher level protocols that are not addressed to a multicast or broadcast address at this sublayer.
HCOutUcastPkts	The number of packets that higher-level protocols requested to be transmitted that are not addressed to a multicast address at this MLT. This total number includes those packets discarded or unsent.
HCInMulticastPkt	The number of packets delivered to this MLT that are addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses.
HCOutMulticast	The total number of packets that higher-level protocols requested be transmitted, and that are addressed to a multicast address at this MLT, including those that are discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
HCInBroadcastPkt	The number of packets delivered to this MLT that are addressed to a broadcast address at this sublayer.
HCOutBroadcast	The total number of packets that higher-level protocols requested to be transmitted, and that are addressed to a broadcast address at this MLT, including those that are discarded or not sent.

Viewing the Ethernet Errors tab

View the Ethernet Errors tab to view read-only statistical information about Ethernet errors that have occurred on the selected Multilink Trunk.

Procedure Steps

Step	Action
1	Open the **MLT_LACP** window by selecting **VLAN, MLT/LACP** from the menu. This window opens with the **VLACP Global** tab selected.
2	Click on **Multilink Trunks** tab.
3	On the Multilink Trunks tab, select the row that represents the MLT to graph and click the **Graph** button. The **MLT Statistics** window opens.

4 Select the **Ethernet Errors** tab.

--End--

Job Aid

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

Field	Description
AlignmentErrors	A count of frames received on a particular MLT that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
FCSErrors	A count of frames received on an MLT that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
IMacTransmitError	A count of frames for which transmission on a particular MLT fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object.
IMacReceiveError	A count of frames for which reception on a particular MLT fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object. The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted.

Field	Description
CarrierSenseErrors	The number of times that the carrier sense condition is lost or never asserted when attempting to transmit a frame on a particular MLT. 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.
FrameTooLong	A count of frames received on a particular MLT that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
SQETestError	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular MLT. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
DeferredTransmiss	A count of frames for which the first transmission attempt on a particular MLT is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollFrames	A count of successfully transmitted frames on a particular MLT for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object.
MultipleCollFrames	A count of successfully transmitted frames on a particular MLT for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.

Field	Description
LateCollisions	The number of times that a collision is detected on a particular MLT later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
ExcessiveColls	A count of frames for which transmission on a particular MLT fails due to excessive collisions.

Network monitoring configuration using Web-based management

This chapter describes the procedure you can use to configure network monitoring using Web-based management.

Navigation

Viewing the system log using Web-based management

Use Web-based management to view the System Log.

Procedure Steps

Step	Action
1	Open the **System Log** window by selecting **Fault, System Log** from the menu.
2	In the **System Log (View By)** section, select the messages you want to display by selecting a value from the **Display Messages From** list.
3	Click **Submit**.

--End--

Clearing the system log in Web-based management

Use Web-based management to clear the System Log.

Procedure steps

Step	Action
1	Open the **System Log** window by selecting **Fault, System Log** from the menu.
2	In the **System Log (View By)** section, select the messages you want to display by selecting a value from the **Display Messages From** list.
3	lear messages from the log by selecting a value from the **Clear Messages From** list.
4	Click **Submit**.

--End--

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

Perform this procedure to retrieve the value of a SNMP object by name or OID.

Step	Action
1	Browse to **Administration**, **Mib Web Page** window.
2	In the **SNMP Object Name/ OID** field, enter the object name or OID.
3	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.
4	Click **Get Next** to retrieve the information of the next object in the MIB. 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	Repeat step 4 as often as required.

--End--

Using the MIB Web page for SNMP walk

Perform this procedure to retrieve the value of a SNMP object by name or OID.

Step	Action
1	Browse to **Administration**, **SNMP Mib Walk** window.
2	In the **SNMP Object Name/ OID** field, enter the object name or OID.
3	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.
4	Click **Next** or **Previous** to view the next or previous twelve objects in the MIB.

--End--

Using the trap Web page to control the generation of traps

Perform this procedure to configure the generation of traps to a certain trap receiver.

Step	Action
1	Browse to **Configuration**, **SNMP Trap** to view the SNMP trap page.
2	In the **Trap Web Page** area, select the trap receiver you want to view.
3	Enable or disable the traps as required.
4	Click **Submit**.

--End--

System diagnostics and statistics using NNCLI

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

Navigation

Port statistics

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

Viewing port-statistics

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

Procedure steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **show port-statistics [port <portlist>]** command.

--End--

Variable Definitions

The following table describes the command parameters.

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

Configuring Stack Monitor

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

Viewing the stack-monitor

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

Procedure Steps

Step	Action
1	Enter Privileged Exec mode.
2	Enter the **show stack monitor** command.

--End--

Job Aid

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

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

Configuring the stack-monitor

Use this procedure to configure the Stack Monitor.

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

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **stack-monitor [enable] [stack-size <2-8>] [trap-interval <30-300>** command.

--End--

Variable Definitions

The following table describes the command parameters.

Variable	Definition
enable	Enables stack monitoring.
stack-size <2-8>	Sets the size of the stack to monitor. Valid range is from 2 to 8. By default the stack size is 2.
trap-interval <30-300>	Sets the interval between traps, in seconds. Valid range is from 30 to 300 seconds. By default the trap-interval is 60 seconds.

Setting default stack-monitor values

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

Configuring default stack monitor using NNCLI

Step	Action
1	Enter Global Configuration mode.
2	Enter the **default stack-monitor** command.

--End--

Disabling the stack monitor

Use this procedure to disable the stack monitor.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **no stack monitor** command.

--End--

Displaying stack health

Use this procedure to display stack health information.

Procedure Steps

Step	Action
1	Enter Privileged Exec mode.
2	Enter the **show stack health** command.

--End--

Job Aid

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

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

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

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

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

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

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

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

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

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

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

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

Viewing Stack Port Counters

Use this procedure to configure the stack port counters.

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

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

Procedure Steps

Step	Action
1	Use the **show stack port-statistics [unit <1-8>]** command to show stacking statistics.
2	Observe the output.

--End--

Variable Definitions

The following table describes the command parameters.

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

Job aid

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

Received	UP	DOWN
Packets	1052	391 283
Multicasts	1052	1582
Broadcasts	0	94
Total Octets	1869077	29862153
Packets 64 bytes	0	389600
65-127 bytes	204	763
128-225 bytes	21	27

Received	UP	DOWN
256-511 bytes	409	492
512-1023 bytes	2	18
1024-1518 bytes	18	19
Jumbo	398	364
Control Packets	0	0
FCS Errors	0	0
Undersized Packets	0	0
Oversized Packets	0	0
Filtered Packets	0	0

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

Clearing stack port counters

Use the following procedure to clear the stack port counters

Procedure Steps

Step	Action
1	Use the **clear stack port-statistics [unit <1-8>]** command to clear stacking statistics.

--End--

Variable Definitions

The following table describes the command parameters.

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

Using the stack loopback test

Use this procedure to complete a stack loopback test

Configuring stack loopback test using NNCLI

Step	Action
1	Enter Privileged Exec mode.
2	Enter the **stack loopback-test internal** command.
3	Observe the NNCLI output.
4	Enter the **stack loopback-test external** command.
5	Observe the NNCLI output.

--End--

Job aid

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

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

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

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

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

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

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

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

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

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

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

Displaying port operational status

Use this procedure to display the port operational status.

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

Procedure Steps

Step	Action
1	Enter Privileged Exec mode.
2	Enter the **show interfaces [port list] verbose** command. If you issue the command with no parameters the port status is shown for all ports.
3	Observe the NNCLI output.

--End--

Validating port operational status

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

VLACP: Configure VLACP on port 1 from a 4500 unit and on port 2 on another 4500 unit. Have a link between these 2 ports. When **show interfaces** command is typed, VLACP status is up for port on the unit where the command is typed. Pull out the link from the other switch, VLACP status goes Down.

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

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

Showing port information

Show port information to show all the configuration information for a specific port in one simple command. The config keyword displays information specific to the port configuration.

Procedure Steps

Step	Action
1	Enter Privileged Exec mode.
2	Enter the **show interfaces <portlist> config** command.
3	Observe the NNCLI output.

--End--

Job aid

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

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

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

Unit/Port: 1/2

```
Trunk:
Admin:  Enable
Oper:  Down
Oper EAP: Up
Oper VLACP: Down
Oper STP: Forwarding
Link:  Down
LinkTrap:  Enabled
Autonegotiation:  Enabled
```

Table 6
VLAN interfaces configuration

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

Table 7
VLAN ID port member configuration

Unit/Port	VLAN	VLAN Name	VLAN	VLAN Name	VLAN	VLAN Name
1/1	256	VLAN #256				
1/2	2	VLAN-2				

Table 8
Spanning-tree port configurations

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

Viewing Environmental status using NNCLI

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

Procedure steps

Step	Action
1	To view the Environmental status of the switch use the following command in the User EXEC mode: **`show environmental`**
	--End--

Job aid

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

```
4548GT-PWR>enable

4548GT-PWR#show environmental
Unit#   PSU1      PSU2   FAN1   FAN2   FAN3   FAN4   Temperature
1       Primary   N/A    OK     OK     OK     OK     OK 33C
2       Primary   N/A    OK     OK     OK     OK     HIGH 41C
4548GT-PWR#
```

System diagnostics and statistics using Device Manager

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

Navigation

Configuring port mirroring with Device Manager

Use the procedure in this section to configure port mirroring using Device Manager.

Procedure Steps

Step	Action
1	Navigate to the port mirror window by choosing **Edit, Diagnostics, Port Mirrors**.
2	Click the **Insert** button
3	Click **Insert**. The window closes and the Port Mirroring window displays the new configuration.
	--End--

Job aid

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

Field	Description
Instance	Numerical assignment of the port mirroring.
Port Mode	The port monitoring mode.
Monitor Port	The port that is the monitoring port.
PortListX	Ports monitored for XrX/Xtx, and manytoOne related mode.
PortListY	Ports monitored for Yrx/Ytx related mode.
MacAddressA	MAC address of the monitored port using Sarc/Adst related mode.
MacAddressB	MAC address of the monitored port using Bsrc/Bdst related mode.

The following table describes the Insert Port Mirrors tab fields.

Field	Description
Instance	Numerical assignment of the port mirroring.
Port Mode	Choose any one of the six port-based monitoring modes or any one of the five address-based monitoring modes. The following options are available: • Adst • Asrc • AsrcBdst • AsrcBdstorBsrcAdst • AsrcorAdst • manytoOneRx • manytoOneRxTx • manytoOneTx • Xrx • XrxorXtx • XrxorYtx • XrxYtx • XrxYtxOrYrxXtx • Xtx The default value is Adst.
Monitor Port	Selects the port that acts as the monitoring port.
PortListX	List of ports to monitor for XrX/Xtx, and manytoOne related mode.
PortListY	List of ports to monitor using Yrx/Ytx related mode.

Field	Description
MacAddressA	MAC address of the port to monitor using Sarc/Adst related mode.
MacAddressB	MAC address of the port to monitor using Bsrc/Bdst related mode.

Configuring Stack Monitor with Device Manager

Use the DM to configure the Stack Monitor.

Procedure Steps

Step	Action
1	Select the chassis.
2	From Device Manager menu bar, select **Edit, Chassis**. The Chassis dialog box appears with the system tab displayed.
3	Click the **Stack Monitor** tab. The Stack Monitor window appears. The following table describes the Stack Monitor tab fields.

Field	Description
StackErrorNotificationEnabled	Enables or disables the Stack Monitoring feature.
ExpectedStackSize	Sets the size of the stack to monitor. Valid range is 2 to 8.
StackErrorNotificationInterval	Sets the interval between traps, in seconds. Valid range is 30 to 300 seconds.

--End--

Display of Environmental status using Device Manager

This section describes the procedures you can perform to view the environmental status of the switch using Device Manager.

Display of Environmental status using Device Manager navigation

- "Viewing the power supply status " (page 84)
- "Viewing the fan status" (page 84)
- "Viewing the temperature" (page 85)

Viewing the power supply status

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

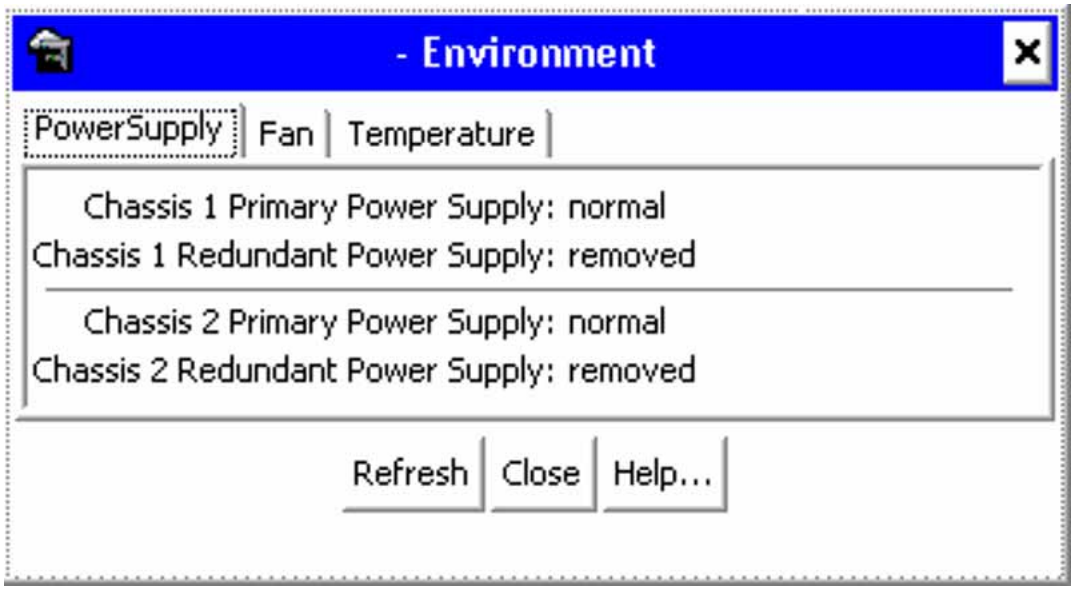
Procedure steps

Step	Action
1	Browse to **Edit**, **Chassis**, **Environment**. The Environment window of the switch appears.
2	Click the **PowerSupply** tab. A report of the power supply status of the switch appears in the Environment window.
3	Click the **Refresh** tab to update the data.

--End--

Job aid

The following screen capture is an example of the PowerSupply status of the switch.



Viewing the fan status

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

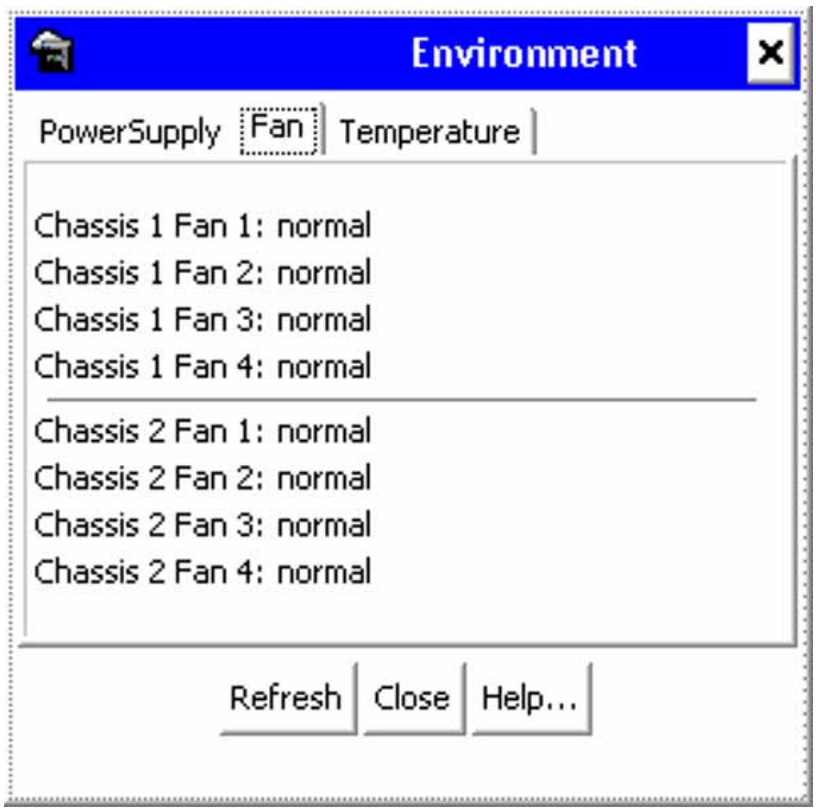
Procedure steps

Step	Action
1	Browse to **Edit**, **Chassis**, **Environment**. The Environment window of the switch appears.
2	Click the **Fan** tab. A report of the status of the Fan appears in the Environment window.
3	Click the **Refresh** tab to update the data.

--End--

Job aid

The following screen capture is an example of the report of the Fan status.



Viewing the temperature

Perform this procedure to view the temperature settings of the switch or stack.

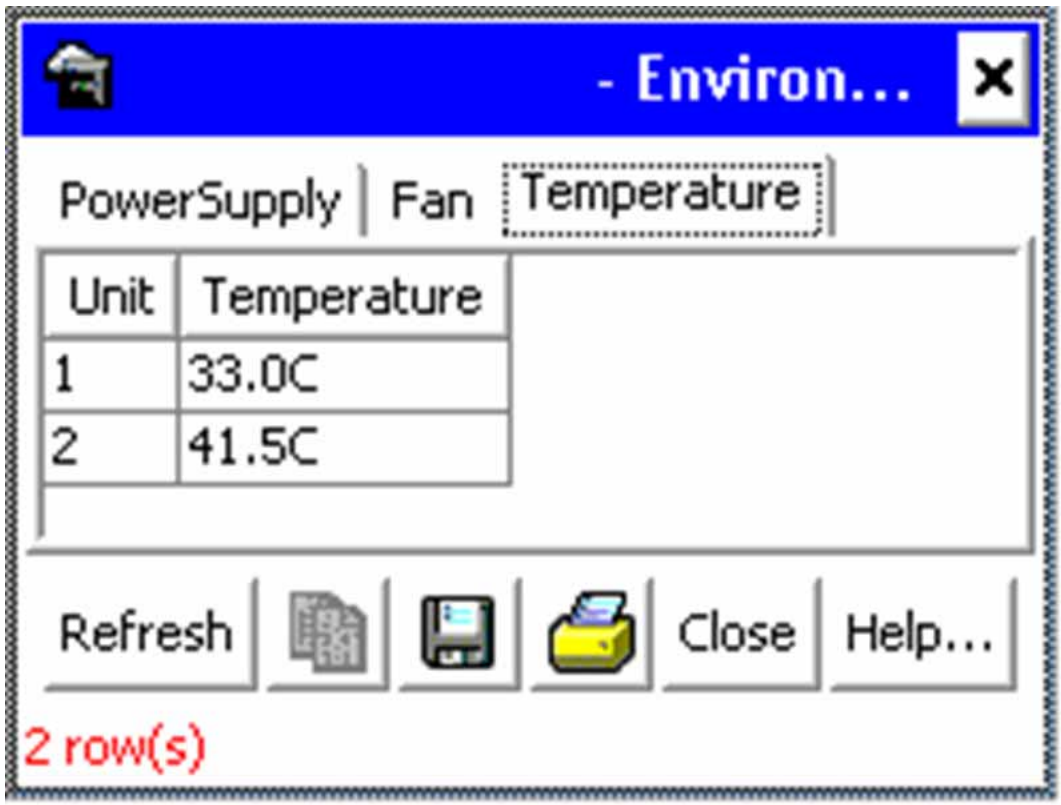
Procedure steps

Step	Action
1	Browse to **Edit**, **Chassis**, **Environment**. The Environment window of the switch appears.
2	Click the **Temperature** tab. A report of the temperature settings of the switch appears in the Environment window.
3	Click the **Refresh** tab to update the data.

--End--

Job aid

The following screen capture is an example of a report of the temperature settings of a switch.



System diagnostics and statistics using Web-based management

This chapter describes the procedures you can use to view diagnostic and statistical information using Web-based management.

Navigation

Configuring port mirroring with Web-based management

Port mirroring can also be configured in Web-based management.

Step	Action
1	Open the **Port Mirroring** window by selecting **Applications, Port Mirroring** from the menu.
2	In the **Port Mirroring Setting** section, enter the new port mirroring settings. The following table describes the fPort Mirroring Setting fields

Field	Description
Monitoring Mode	Choose any one of the six port-based monitoring modes or any one of the five address-based monitoring modes. The following options are available: • Disabled • -> Port X • Port X ->\n• <-> Port X • -> Port X or Port Y ->\n• -> Port X and Port Y ->\n• <-> Port X and Port Y <-> • Address A -> any Address • any Address -> Address A • <-> Address A • Address A -> Address B • Address A <-> Address B The default value is Disabled.
Monitor Port	Select the port that acts as the monitoring port.

3 Click **Submit**.

The new mirroring configuration is displayed in Port Mirroring Active section.

--End--

Stack health check

You can observe the stack health through Web management. The information is presented is a similar fashion as the NNCLI output.

Procedure Steps

Step	Action
1	Navigate to **Summary, Stack Health**.
2	The browser displays the stack health information.

--End--

Viewing port statistics

Use this procedure to view statistical data about a selected port.

Procedure Steps

Step	Action
1	Select a port from the **Port** list in the **Port Statistics (View By)** section.
2	Open the **Port Statistics** window by selecting **Statistics, Port** from the menu.
3	Click **Submit**.
4	Click **Update** to refresh the statistical information.
5	Click **Zero Port** to reset the counters for the selected port.
6	Click **Zero All Ports** to reset the counters for all ports.

--End--

Port statistics are displayed in the Port Statistics Table section.

The following table describes the fields in the port statistics section.

Field	Description
Packets	The number of packets received/transmitted on this port, including bad packets, broadcast packets, and multicast packets.
Multicast	The number of good multicast packets received/transmitte d on this port, excluding broadcast packets.
Broadcasts	The number of good broadcast packets received/transmit ted on this port.
Total Octets	The number of octets of data received/transmitted on this port, including data in bad packets and FCS octets, and framing bits.
Pause Frames	The number of pause frames received/transmitted on this port.
FCS-Frame Errors	The number of valid-size packets received on this port with proper framing but discarded because of FCS or frame errors.
Undersized Packets	The number of packets received on this port with fewer than 64 bytes and with proper CRC and framing (also known as short frames or runts).

Field	Description
Oversized Packets	The number of packets that are received on this port with proper CRC and framing that meet the following requirements: • 1518 bytes if no VLAN tag exists • 1522 bytes if a VLAN tag exists
Filtered Packets	The number of packets that are received on this port and discarded because of the specific configuration. This counter does not count the FCS/Frames error packets; they are counted in FCS/Frames error counter. The filtered packets counter counts packets discarded because STP is not set to forwarding, the frame setting in VLAN directs discarding, or a mismatch, in ingress/egress port speeds.
Collisions	The number of collisions detected on this port.
Single Collisions	The number of packets that are transmitted successfully on this port after a single collision.
Multiple Collisions	The number of packets that are transmitted successfully on this port after more than one collision.
Excessive Collisions	The number of packets lost on this port due to excessive collisions.
Late Collisions	The number of packets collisions that occurred after a total length of time that exceeded 512 bit-times of packet transmission.
Deferred Packets	The number of packets that are received on this port are delayed on the first transmission attempt, but never incurred a collision.
Packets 64 bytes 65-127 bytes 128-255 bytes 256-511 bytes 512-1023 bytes 1024-1518 bytes 1519-9216 bytes(Jumbo_	The number of packets received/transmitted on the port.

Viewing all port errors

View all port errors to view a summary of the port errors.

Step	Action
1	Open the **Port Error Summary** window by selecting **Statistics, Port Error Summary** from the menu. The following table describes the Port Error Summary.

Field	Description
Unit	Displays the unit number in the stack.
Port	Displays the port number of the unit.
Status	Displays the status of the port (Enabled/Disabled).
Link	Displays the link status of the port (Up/Down).
Speed/Duplex	Displays the speed at which the port is operating, as well as whether it is in half- or full-duplex mode.
FCS/Frame Errors	Displays the number of frame check sequence (FCS) and frame errors received on this port.
Collisions	Displays the number of collisions errors received on this port.
Single Collisions	Displays the number of single collisions errors received on this port.
Multiple Collisions	Displays the number of multiple collisions errors received on this port.
Excessive Collisions	Displays the number of excessive collisions errors received on this port.
Late Collisions	Displays the number of late collisions errors received on this port.

2	Click **Update** to refresh the statistical information.

--End--

Viewing interface statistics

To view statistical information for an interface, perform the following procedure.

Step	Action
1	Open the **Interface Statistics** window by selecting **Statistics, Interface** from the menu. The following table describes the fields on this window. The following table describes the Interface Statistics fields.

Table 9
Field Descriptions

Field	Description
Port	The port number corresponding to the selected switch.
In Octets	The number of octets received on the interface, including framing characters.
Out Octets	The number of octets transmitted out of the interface, including framing characters.
In Unicast	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Out Unicast	The number of packets that higher-layer protocols requested to be transmitted to a subnetwork-unicast address, including those that are discarded or not sent.
In Non-Unicast	The number of nonunicast packets, for example, subnetwork-broadcast or subnetwork-multicast packets, delivered to a higher protocol.
Out Non-Unicast	The number of packets that higher-level protocols requested to be transmitted to a nonunicast address. For example, a subnetwork-broadcast or a subnetwork multicast address, including those that are discarded or not sent.
In Discards	The number of inbound packets which are selected to be discarded even though no errors are detected to prevent their being delivered to a higher-layer protocol. Packet discarding is not arbitrary. One reason for discarding packets is to free buffer space.
Out Discards	The number of outbound packets selected to be discarded even though no errors are detected to prevent their being transmitted. Packet discarding is not arbitrary. One reason for discarding packets is to free up buffer space.
In Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Out Errors	The number of outbound packets that cannot be transmitted because of errors.
In Unknown Protos	The number of packets received through the interface that are discarded because of an unknown or unsupported protocol.

2 Click **Update** to refresh the statistical information.

--End--

Viewing Ethernet error statistics

Use this procedure to view Ethernet error statistics.

Step	Action
1	Open the **Ethernet Errors** window by selecting **Statistics, Ethernet Errors** from the menu. The following table describes the Ethernet Errors fields.

Table 10
Ethernet Error fields

Field	Description
Port	The port number corresponding to the selected switch.
FCS/Frame Errors	The number of frames received on a particular interface that are an integral number of octets in length, but do not pass the FCS check or have frame errors.
Internal MAC Transmit Errors	The number of frames for which transmission on a particular interface fails because of an internal MAC sublayer transmit error. A frame only is counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.
Internal MAC Receive Errors	The number of frames for which reception on a particular interface fails because of an internal MAC sublayer transmit error. A frame only is counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.
Carrier Sense Errors	The number of times that the carrier sense conditions are lost or never asserted when attempting to transmit a frame on a particular interface.
SQE Test Errors	The number of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR 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.
Deferred Transmissions	The number of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.
Single Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.

Field	Description
Multiple Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by a single collision.
Late Collisions	The number of times a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.
Excessive Collisions	The number of frames for which transmission on a particular interface fails due to excessive collisions.

2 Click **Update** to refresh the statistical information.

--End--

Viewing transparent bridging statistics

Use this procedure to To view transparent bridging statistics.

Step	Action
1	Open the **Transparent Bridging** window by selecting **Statistics, Transparent Bridging** from the menu. The following table describes the transparent bridging statistics fields.

Table 11
Transparent Bridging window

Field	Description
Port	The port number that corresponds to the selected switch.
In Frames (dot1dTpPortInFrames)	The number of frames received by this port from its segment. A frame received on the interface corresponding to this port is counted only if it is for a protocol being processed by the local bridging function, including bridge management errors.
Out Frames (dot1dTpPortOutFrames)	The number of frames transmitted by this port from its segment. A frame transmitted on the interface corresponding to this port is counted only if it is for a protocol being processed by the local bridging function, including bridge management errors.
In Discards (dot1dTpPortInDiscards)	The number of valid frames received which are discarded by the forwarding process.

2 Click **Update** to refresh the statistical information.

--End--

Monitoring MLT traffic

Use this procedure to monitor bandwidth usage for the Multilink Trunk (MLT) member ports within each trunk in a configuration by selecting the traffic type to monitor.

Procedure Steps

Step	Action
1	Open the **MLT Utilization** window by selecting **Applications, MultiLink Trunk, Utilization** from the menu. The **MultiLink Trunk Utilization Table** section is be populated with information. The following table describes the fields in this table.

Table 12
MultiLink Trunk Utilization Table fields

Field	Description
Unit/Port	A list of the trunk member switch ports that correspond to the trunk specified in the Trunk column.
Last 5 Minutes	The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last five minutes. This field provides a running average of network activity, and is updated every 15 seconds.
Last 30 Minutes	The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last 30 minutes. This field provides a running average of network activity, and is updated every 15 seconds.
Last Hour	The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last 60 minutes. This field provides a running average of network activity, and is updated every 15 seconds.

2 In the **MultiLink Trunk Utilization Selection (View By)** area, select a trunk to monitor in the **Trunk** list and a type of traffic in the **Traffic Type** list.

3 Click **Submit**.

--End--

RMON configuration using the NNCLI

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

Navigation

Viewing the RMON alarms

Use this procedure to display information about RMON alarms.

Procedure Steps

Step	Action
1	Enter Global Configuration mode
2	Enter the **`show rmon alarm`** command.

3	Observe the NNCLI output.

--End--

Viewing the RMON events

Use this procedure to display information regarding RMON events.

Procedure Steps

Step	Action
1	Enter Global Configuration mode
2	Enter the **show rmon event** command.
3	Observe the NNCLI output.

--End--

Viewing the RMON history

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

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **show rmon history** command.
3	Observe the NNCLI output.

--End--

Viewing the RMON statistics

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

Procedure Steps

Step	Action
1	Enter Global Configuration mode
2	Enter the **show rmon stats** command.

3 Observe the NNCLI output.

--End--

Configuring RMON alarms

Use this procedure to set RMON alarms and thresholds.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **rmon alarm <1-65535> <WORD> <1-2147483647> {absolute | delta} rising-threshold <-2147483648-2147483647> [<1-65535>] falling-threshold <-2147483648-2147483647> [<1-65535>] [owner <LINE>]** command.
3	Observe the command output.

--End--

Variable Definitions

The following table describes the command parameters.

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

Variable	Definition
falling-threshold <-2147483648-2147483647 > [<1-65535>]	The first integer value is the falling threshold value. The optional second integer specifies the event entry to be triggered when the falling threshold is crossed. If omitted, or if an invalid event entry is referenced, no event is triggered. Unique index for the alarm entry.
[owner <LINE>]	Specify an owner string to identify the alarm entry.

Deleting RMON alarms

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

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **no rmon alarm [<1-65535>]** command.
3	Observe the NNCLI output.

--End--

Variable Definitions

The following table describes the command parameters.

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

Configuring RMON events settings

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

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **rmon event <1-65535> [log] [trap] [description <LINE>] [owner <LINE>]** command.
3	Observe the NNCLI output.

--End--

Variable Definitions

The following table describes the command parameters.

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

Deleting RMON events settings

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

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **no rmon alarm [<1-65535>]** command.
3	Observe the NNCLI output.

--End--

Variable Definitions

The following table describes the command parameters.

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

Configuring RMON history settings

Use this procedure to configure RMON history settings.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **rmon history <1-65535> <LINE> <1-65535> <1-3600> [owner <LINE>]** command.

3 Observe the NNCLI output.

--End--

Variable Definitions

The following table describes the command parameters.

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

Deleting RMON history settings

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

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the `no rmon history [<1-65535>]` command.
3	Observe the NNCLI output.

--End--

Variable Definitions

The following table describes the command parameters.

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

Configuring RMON statistics settings

Use this procedure to configure RMON statistics settings.

Configuring RMON statistics settings using NNCLI

Step	Action
1	Enter Global Configuration mode.
2	Enter the **rmon stats <1-65535> <LINE> [owner <LINE>]** command.
3	Observe the NNCLI output.

--End--

Variable Definitions

The following table describes the command parameters.

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

Deleting RMON statistics settings

Use this procedure to turn off RMON statistics. When omit the variable all entries in the table are cleared.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **no rmon stats [<1-65535>]** command.
3	Observe the NNCLI output.

--End--

Variable Definitions

The following table describes the command parameters.

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

RMON configuration using Device Manager

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

Navigation

Working with RMON information

This section describes the procedures you can use to view RMON information by looking at the graphing information associated with the port or chassis.

Navigation

Viewing RMON statistics using the DM

Use this procedure to gather Ethernet statistics that can be graphed in a variety of formats or saved to a file that can be exported to an outside presentation or graphing application.

Procedure Steps

Step	Action
1	Select a port from the initial DM window.
2	The **Graph Port** window opens. Click the **RMON** tab.
3	Do one of the following: **a** From the shortcut menu, choose **Graph**. **b** Select **Graph, Port** from the menu. **c** On the toolbar, click the **Graph** button.

--End--

Job Aid

The following table describes the fields on the RMON tab.

Field	Descriptions
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
BroadcastPkts	The total number of good packets received that are directed to the broadcast address. This does not include multicast packets.
MulticastPkts	The total number of good packets received that are directed to a multicast address. This number does not include packets directed to the broadcast address.
CRCAlignErrors	The total number of packets received that have a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but have either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
UndersizePkts	The total number of packets received that are less than 64 octets long (excluding framing bits but including FCS octets) and are otherwise well formed.
OversizePkts(>1518)	The total number of packets received that are longer than 1518 octets (excluding framing bits but including FCS octets) and are otherwise well formed.

Field	Descriptions
Fragments	The total number of packets received that are less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). It is entirely normal for etherStatsFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Jabbers	The total number of packets received that are longer than 1518 octets (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 milliseconds (ms). The allowed range to detect jabber is between 20 ms and 150 ms.
1..64	The total number of packets (including bad packets) transmitted and received on this port between 1 and 64 octets in length (excluding framing bits but including FCS octets).
65..127	The total number of packets (including bad packets) transmitted and received on this port between 65 and 127 octets in length (excluding framing bits but including FCS octets).
128..255	The total number of packets (including bad packets) transmitted and received on this port between 128 and 255 octets in length (excluding framing bits but including FCS octets).
256..511	The total number of packets (including bad packets) transmitted and received on this port between 256 and 511 octets in length (excluding framing bits but including FCS octets).
512..1023	The total number of packets (including bad packets) transmitted and received on this port between 512 and 1023 octets in length (excluding framing bits but including FCS octets).
1024..1518	The total number of packets (including bad packets) transmitted and received on this port between 1024 and 1518 octets in length (excluding framing bits but including FCS octets).

Statistic	Description
Poll Interval	Statistics are updated based on the poll interval. Default: 10 seconds (s) Range: None, 2s, 5s, 10s, 30s, 1 minutes(m), 5m, 30m 1 hour (h)
Absolute	The total count since the last time counters are reset. A system reboot resets all counters.
Cumulative	The total count since the statistics tab is first opened. The elapsed time for the cumulative counter is shown at the bottom of the graph window.

Statistic	Description
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/sec	The average for the counter over the last polling interval.

Viewing RMON history

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

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

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

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

Use the following procedure to view RMON history:

Step	Action
1	Open the **RmonControl** window by selecting **RMON, Control** from the menu.
2	Observe the RMON control window.

--End--

Disabling RMON history

Use this procedure to disable RMON history on a port.

Procedure Steps

Step	Action
1	Open the **RmonControl** window by selecting **RMON, Control** from the menu.
2	Highlight the row that contains the record to delete.

3 Click **Delete**.

--End--

Viewing RMON history statistics

Us this procedure to display RMON history statistics:

Procedure Steps

Step	Action
1	Open the **RmonControl** window by selecting **RMON, Control** from the menu.
2	Select a port in the **RMON History** tab.
3	Click **Graph**.
4	The **RMON History** window opens for the selected port.

--End--

Job Aid

The following table describes the RMON History tab fields.

Field	Description
SampleIndex	The sample number. As history samples are taken, they are assigned greater sample numbers.
Utilization	Estimate the percentage of the capacity of a link that is used during the sampling interval.
Octets	The number of octets received on the link during the sampling period.
Pkts	The number of packets received on the link during the sampling period.
BroadcastPkts	The number of packets received on the link during the sampling interval that destined for the packet address.
MulticastPkts	The number of packets received on the link during the sampling interval that are destined for the multicast address. This does not include the broadcast packets.
DropEvents	The number of received packets that are dropped because of system resource constraints.
CRCAlignErrors	The number of packets received during a sampling interval that are between 64 and 1518 octets long. This length includes Frame Check Sequence (FCS) octets but not framing bits. The packets had a bad FCS with either an integral number of octets (FCS Error) or a nonintegral number of octets (Alignment Error).

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

Enabling Ethernet statistics gathering

Use this procedure to gather Ethernet statistics.

Procedure Steps

Step	Action
1	Open the **RmonControl** window by selecting **RMON, Control** from the menu.
2	Enter the owner of this RMON entry in the **Owner** field.
3	Select the **Ether Stats** tab.
4	Click **Insert**. The **Insert Ether Stats** window opens.
5	Enter the ports to be used. Port numbers can be manually entered into the **Port** field or selected by clicking the ellipsis (...) and using the **Port List** window to make the selections.
6	Click **Insert**.

--End--

Job Aid

The following table describes the Ether Stats tab fields.

Table 13
Ether Stats tab fields

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

Disabling Ethernet statistics gathering

Use this procedure to disable Ethernet statistics.

Procedure Steps

Step	Action
1	Open the **RmonControl** window by selecting **RMON,Control** from the menu.
2	Select the **Ether Stats** tab.
3	Highlight the row that contains the record to delete.
4	Click **Delete**.

--End--

Using Alarm Manager

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

Navigation

- "Creating an alarm" (page 111)
- "Deleting an alarm" (page 113)

Creating an alarm

To create an alarm to receive statistics and history using default values:

Procedure Steps

Step	Action
1	Open the **Alarm Manager** window by selecting **RMON, Alarm Manager** from the menu. This window is illustrated below.
2	In the **Variable** field, select a variable and a port (or other ID) from the list to set the alarm.

Alarm variables are in the three following formats, depending on the type:

- A chassis alarm ends in .x where the x index is hard-coded. No further information is required.
- A card, spanning tree group (STG) or EtherStat alarm ends with a dot (.). You must enter a card number, STG ID, IP address, or EtherStat information.
- A port alarm ends with no dot or index and requires using the port shortcut menu. An example of a port alarm is ifInOctets (interface incoming octet count).

3 In the remaining fields, enter the information for the alarm.

4 Click **Insert**.

--End--

Job Aid

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

Table 14
RMON Insert Alarm dialog box fields

Field	Description	
Variable	Name and type of alarm—indicated by the format: • *alarmname.x* where x=0 indicates a chassis alarm. • *alarmname*. where you must specify the index. This is a card number for module-related alarms, an STG ID for spanning tree group alarms (the default STG is 1, other STG IDs are user-configured), or the Ether Statistics Control Index for RMON Stats alarms. • *alarmname* with no dot or index is a port-related alarm and displays in the port selection tool.	
Sample Type	Can be either absolute or delta. .	
Sample Interval	Time period (in seconds) over which the data is sampled and compared with the rising and falling thresholds.	
Index	Uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device.	
Threshold Type	**Rising Value**	**Falling Value**

Field	Description	
Value	When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, generates a single event.	When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, generates a single event.
Event Index	Index of the event entry that is used when a rising threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already filled in.)	Index of the event entry that is used when a falling threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already filled in.)

Deleting an alarm

Use this procedure to delete an alarm:

Procedure Steps

Step	Action
1	Open the **Alarms** window by selecting **RMON, Alarms** from the menu.
2	Select the alarm you want to delete.
3	Click **Delete**.

--End--

Job Aid

The following table describes the alarm tab fields.

Field	Description
Index	Uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device.
Interval	The interval in seconds over which data is sampled and compared with the rising and falling thresholds. When setting this variable, note that in the case of deltaValue sampling, you are to set the interval short enough so the sampled variable is unlikely to increase or decrease by a delta of more than 2^31 - 1 during a single sampling interval.
Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Counter, Gauge, or TimeTicks) can be sampled.

Field	Description
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue(2), the value of the selected variable at the last sample is subtracted from the current value, and the difference is compared with the thresholds.
Value	The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value is the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value is the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds. The value during the current sampling period is not made available until the period is complete and it remains available until the next period is complete.
StartupAlarm	The alarm that may be sent when this entry is first set to Valid. If the first sample after this entry that becomes valid is greater than or equal to the risingThreshold and the alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3), a single rising alarm is generated. If the first sample after this entry that becomes valid is less than or equal to the fallingThreshold and the alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3), a single falling alarm is generated.
RisingThreshold	A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3). After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold.
RisingEventIndex	The index of the eventEntry that is used when a rising threshold is crossed. The eventEntry identified by a particular value of this index is the same as that identified by the same value of the eventIndex object. If there is no corresponding entry occurs in the eventTable, no association exists. In particular, if this value is zero, no associated event is generated because zero is not a valid event index.
FallingThreshold	A threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold and the associated alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3). After a falling event is generated, another such event is not generated until the sampled value rises above this threshold and reaches the alarmRisingThreshold.

Field	Description
FallingEventIndex	The index of the eventEntry that is used when a falling threshold is crossed. The eventEntry identified by a particular value of this index is the same as that identified by the same value of the eventIndex object. If no corresponding entry in the eventTable, then no association exists. In particular, if this value is zero, no associated event is generated because zero is not a valid event index.
Owner	The network management system that creates this entry.
Status	The status of this alarm entry.

Using Events

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

Navigation

- “Viewing an event” (page 115)
- “Creating an event” (page 116)
- “Deleting an event” (page 117)

Viewing an event

To view a table of events, perform the following procedure.

Procedure Steps

Step	Action
1	Open the **Alarms** window by selecting **RMON, Alarms** from the menu.
2	Select the **Events** tab.

--End--

Job Aid

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

Table 15
Events tab fields

Field	Description
Index	This index uniquely identifies an entry in the event table. Each entry defines one event that is to be generated when the appropriate conditions occur.
Description	Specifies whether the event is a rising or falling event.
Type	The type of notification that the switch provides about this event. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations. Possible notifications follow: • none • log • trap • log-and-trap
Community	The SNMP community string acts as a password. Only those management applications with this community string can view the alarms.
LastTimeSent	The value of sysUpTime at the time this event entry last generated an event. If this entry has not generates any events, this value is zero.
Owner	If traps are specified to be sent to the owner, this is the name of the machine that receives alarm traps.

Creating an event

To create an event, perform the following procedure.

Procedure Steps

Step	Action
1	Open the **Alarms** window by selecting **RMON, Alarms** from the menu.
2	Select the **Events** tab.
3	Click **Insert**. The **Insert Events** window opens.
4	In the **Description** field, type a name for the event.
5	Select the type of event in the **Type** field.
6	Enter the community information in the **Community** field.
7	Enter the owner information in the **Owner** field.
8	Click **Insert**.

--End--

Deleting an event

Use this procedure to delete an event.

Procedure Steps

Step	Action
1	Open the **Alarms** window by selecting **RMON, Alarms** from the menu.
2	Select the **Events** tab.
3	Select an event from the list.
4	Click **Delete**.

--End--

Using log information

The **Log** tab to chronicle and described the alarm activity.

Procedure Steps

Step	Action
1	Open the **Alarms** window by selecting **RMON, Alarms** from the menu.
2	Select the **Log** tab.

--End--

Job Aid

The following table describes the Log tab fields.

Table 16
Log tab fields

Item	Description
Time	Specifies when an event occurs that activats the log entry.
Description	Specifies whether the event is a rising or falling event.

RMON configuration using Web-based management

This chapter describes the procedures you can use to configure and manage RMON using Web-based management.

Navigation

Configuring RMON fault threshold parameters

You can configure alarms to alert you when the value of a variable goes out of range. RMON alarms can be defined on any MIB variable that resolves to an integer value. You cannot use alarm variables as string variables.

Creating an RMON fault threshold

To configure an RMON fault threshold, perform the following procedure.

Procedure Steps

Step	Action
1	Open the **RMON Threshold** window by selecting **Fault, RMON Threshold** from the menu.
2	In the fields provided in the **RMON Threshold Creation** section, enter the information for the new threshold.
3	Click **Submit**.

--End--

Job Aid

The following table describes the fields in RMON threshold..

Field	Description
Alarm Index	Unique number to identify the alarm entry.
Port	The port on which to set an alarm.
Parameter	The sampled statistic.
Rising Level	The event entry to be used when a rising threshold is crossed.
Falling Level	The event entry to be used when a falling threshold is crossed.
Rising Action	The type of notification for the event. Selecting Log generates an entry in the RMON Event Log table for each event. Selecting SNMP Trap sends an SNMP trap to one or more management stations.
Interval	The time period (in seconds) to sample data and compare the data to the rising and falling thresholds.
Alarm Sample	The sampling method: • Absolute: *Absolute* alarms are defined on the current 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. Therefore, an alarm could be created with a rising value of 2 and a falling value of 1 to alert a user to whether the card is up or down. • Delta: 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. Therefore, if you keep track of the current values of a given delta-valued alarm and add them together, the result is twice the actual value. (This result is not an error in the software.)

Deleting RMON threshold configuration

Use this procedure to delete an existing RMON threshold configuration.

Procedure Steps

Step	Action
1	Open the **RMON Threshold** window by selecting **Fault, RMON Threshold** from the menu.

2 In the **RMON Threshold Table**, click the **Delete** icon in the row of the entry you want to delete.
A message prompts for confirmation of the request.

3 Click **Yes**.

--End--

Viewing the RMON fault event log

Use the following procedure to view a history of RMON fault events.

Procedure Steps

Step	Action
1	From the menu, select **Fault, RMON Event Log** to open the **RMON Event Log** window.
2	The **RMON Event Log** displays.

--End--

Nortel Ethernet Routing Switch 4500 Series

Configuration — System Monitoring

Release: 5.3
Publication: NN47205-502
Document revision: 05.01
Document release date: 27 April 2009

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com
Sourced in Canada