Nortel Ethernet Routing Switch 5000 Series

Configuration — System Monitoring

Release: 6.1
Document Revision: 05.01

www.nortel.com

NN47200-505

Nortel Ethernet Routing Switch 5000 Series
Release: 6.1
Publication: NN47200-505
Document release date: 25 May 2009

Contents

New in this release

The following sections detail what's new in *Nortel Ethernet Routing Switch 5000 Series Configuration — System Monitoring* (NN47200-505) for Release 6.1.

Features

See the following sections for information about feature changes:

- "Stack Health Check" (page 9)
- "Stack environmental information" (page 9)

Stack Health Check

The Stack Health Check feature provides information on the stacking state of each switch rear port. It is used to run a high-level test to monitor the rear port status for each unit, confirm the number of switching units in stack, detect if the stack runs with a temporary base unit, and to monitor stack continuity. For more information, see:

- "Stack Health Check" (page 29)
- "Showing stack health information" (page 40)
- "Viewing stack health" (page 53)

Stack environmental information

This feature provides information on the status of the environment of each unit in a stack. For more information, see:

- "Displaying environmental information" (page 30)
- "Viewing environmental information" (page 43)

Introduction

This document provides information you need to configure and use system monitoring for the Ethernet Routing Switch 5000 Series.

NNCLI command modes

NNCLI provides the following command modes:

- User Executive
- Privileged Executive
- Global Configuration
- Interface Configuration
- Router Configuration

Mode access is determined by access permission levels and password protection.

If no password is set, you can enter NNCLI in User Executive mode and use the **enable** command to move to the next level (Privileged Executive mode). However, if you have read-only access, you cannot progress beyond User Executive mode, the default mode. If you have read-write access you can progress from the default mode through all of the available modes.

With sufficient permission, you can use the rules in the following table to move between the command modes.

Table 1
NNCLI command modes

Command mode and sample prompt	Entrance commands	Exit commands
User Executive ERS5000>	No entrance command, default mode	**exit** or **logout**

Command mode and sample prompt	Entrance commands	Exit commands
Privileged Executive `ERS5000#`	**`enable`**	**`exit`** or **`logout`**
Global Configuration `ERS5000(config)#`	From Privileged Executive mode, enter: **`configure`**	To return to Privileged Executive mode, enter: **`end`** or **`exit`** To exit NNCLI completely, enter: **`logout`**
Interface Configuration `ERS5000(config-if)#`	From Global Configuration mode: To configure a port, enter: interface fastethernet <port number> To configure a VLAN, enter: interface vlan <vlan number>	To return to Global Configuration mode, enter: **`exit`** To return to Privileged Executive mode, enter: **`end`** To exit NNCLI completely, enter: **`logout`**
Router Configuration `ERS5000(config-router)#`	From Global Configuration mode: To configure router OSPF, type: **`router ospf`** To configure router RIP, type: **`router rip`** To configure router VRRP, type: **`router vrrp`**	To return to Global Configuration mode, enter: **`exit`** To return to Privileged EXEC mode, type: **`end`** To exit NNCLI completely, type: **`logout`**

See *Nortel Ethernet Routing Switch <2500/4500/5000> Series Fundamentals* <NN47215-102/NN47205-102/NN47200-104>

Navigation

System monitoring fundamentals

System monitoring is an important aspect of switch operation. The Nortel Ethernet Routing Switch 5500 Series provides a wide range of system monitoring options that you can use to closely monitor the operation of a switch or stack.

This chapter describes two general system monitoring aspects that you must consider when you use the Ethernet Routing Switch 5000 Series: system logging and port mirroring. Subsequent chapters provide information about specific system monitoring tools and how to use them.

System logging

The Nortel Ethernet Routing Switch 5500 Series supports system logging (syslog), a software tool to log system events for debugging and analysis.

The syslog tool can log application events. The logged events are stored in volatile RAM, nonvolatile RAM, or in a remote host. You can select the storage location by using the Nortel Networks command line interface (NNCLI) or DM.

Remote logging

Starting with release 5.0, the remote logging feature provides an enhanced level of logging by replicating system messages on a syslog server. System log messages from several switches can be collected at a central location to alleviate you from individually querying each switch to interrogate the log files.

You must configure the remote syslog server on the unit to log informational, serious, and critical messages to this remote server. The 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 is captured the system stores up to 10 messages that are sent after the IP address of the remote server is on the system.

To configure this feature, enable remote logging, specify the IP address of the remote syslog server, and specify theseverity level of the messages to be sent to the remote server.

Alarms

Alarms are useful for identifying values of a variable that have gone out of range. Define an RMON alarm for a MIB variable that resolves to an integer value. String variables cannot be used. All alarms share the following characteristics:

- An upper and lower threshold value is defined.
- A corresponding rising and falling event occurs.
- An alarm interval or polling period is reached.

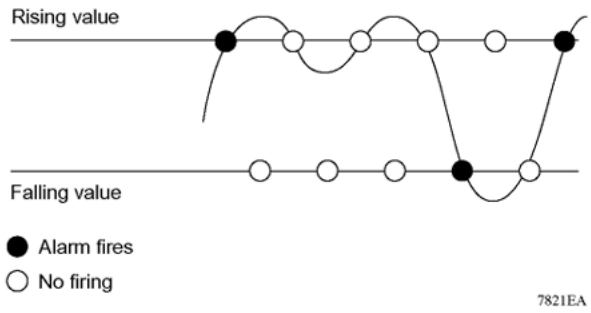
After alarms are activated, view the activity in a log or a trap log, or a script can be created to provide notification by beeping a console, sending e-mail messages, or calling a pager.

How RMON alarms work

The alarm variable is polled and the result is compared against upper and lower limit values you select after you create the alarm. If either limit is reached or crossed during the polling period; then the alarm fires 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 fires as a rising event. During the first interval that the data drops below the falling value, the alarm fires as a falling event.

The following figure describes how alarms fire.



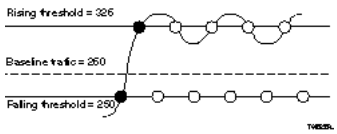
The alarm fires during the first interval that the sample goes out of range. No additional events are generated for that threshold until the opposite threshold is crossed. Therefore, it is important to carefully define the rising and falling threshold values for alarms to work as expected. Otherwise,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

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

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

If the alarm is defined with a falling threshold less than 260 (assuming the alarm polling interval is 10 seconds) the rising alarm can fire only once. For the rising alarm to fire a second time, the falling alarm (the opposite threshold) must fire. Unless the port becomes inactive or spanning tree is disabled (which will 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.

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



Creating alarms

Select a variable from the variable list and a port, or other switch component, to which it is connected. Some variables require port IDs, card IDs, or other indices (for example, spanning tree group IDs). Then select a rising and a falling threshold value. The rising and falling values

are compared against the actual value of the variable that you choose. If the variable falls outside of the rising or falling value range, an alarm is triggered and an event is logged or trapped.

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

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

Trap Web page

SNMP Trap web page provides a graphical method to enable or disable traps you want to send. In case multiple trap receivers are selected you can specify which traps are sent to which receiver. The selection of traps to be sent to a certain receiver can be based on criteria like security, network connectivity, or other information that might be 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. The access to those pages is 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.

Management Information Base 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:

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

IGMP and the system event log

IGMP uses the components provided by the syslog tool. The syslog tool performs functions, such as storing messages in the NVRAM or remote host and displaying these log messages through the NNCLI, console menu, or Telnet.

The IGMP log events can be in one of the following three categories based on their severity:

- Critical
- Serious
- Informational

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

- IGMP initialization
- Configuration changes from the user
- Stack Join events
- IGMP messages: Report, Leave and Query messages received by the switch

Events such as reception of IGMP messages occur frequently in the switch whenever a new host joins or leaves a group. Logging such messages consumes a large amount of log memory.

Therefore, such messages should not be logged in all the time. By default, such message logging is disabled. You must enable this feature through the NNCLI to view the messages.

In Table 2 " IGMP syslog messages" (page 20):

- %d represents a decimal value for the preceding parameter. For example, 5 for VLAN 5
- %x represents a hexadecimal value for the preceding parameter. For example, 0xe0000a01 for Group 224.0.10.1

Table 2 " IGMP syslog messages" (page 20) describes the IGMP syslog messages and the 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
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

Table 2
IGMP syslog messages (cont'd.)

Severity	Log messages
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

Port mirroring

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

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

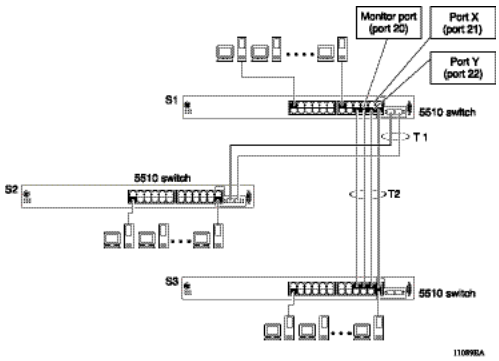
Port-based mirroring configuration

Figure 1 "Port-based mirroring example" (page 22) 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), any trunk member of T1 and T2 can also be monitored.

In this example, Figure 1 "Port-based mirroring example" (page 22) 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.

You cannot monitor trunks and you cannot configure trunk members as monitor ports.

Figure 1
Port-based mirroring example



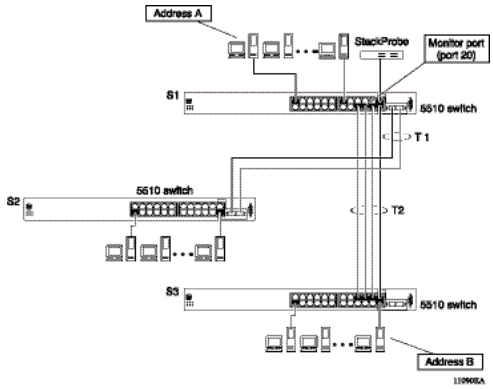
In the preceding configuration example , you can configure the designated monitor port (port 20) to monitor traffic in any of the following modes:

- 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 or transmitted by port X and transmitted or received by port Y (conversations between port X and port Y).
- Monitor all traffic received on many ports.
- Monitor all traffic transmitted on many ports.
- Monitor all traffic received or transmitted on many ports.

Address-based mirroring configuration

The following example shows 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 2
Address-based mirroring example



In this configuration, the designated monitor port (port 20) can be set 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).

Many-to-Many Port Mirroring

Many-to-Many Port Mirroring is an extension of the Port Mirroring application, to allow multiple sessions of mirroring configuration to exist simultaneously, each with a Monitor Port and mirrored ports.

You can configure this the feature by using NNCLI or Web-based management. The configuration process for each instance is similar to Port Mirroring configuration.

Port-based modes

The following port-based modes are supported:

- **ManytoOneRx**: Many-to-One port mirroring on ingress packets.
- **ManytoOneTx**: Many to one port mirroring on egress packets.
- **ManytoOneRxTx** Many to one port mirroring on ingress and egress traffic.
- **Xrx**: Mirror packets received on port X.
- **Xtx**: Mirror packets transmitted on port X.

- **XrxOrXtx**: Mirror packets received or transmitted on port X.
- **XrxYtx**: Mirror packets received on port X and transmitted on port Y.
- **XrxYtxOrYrxXtx**: Mirror packets received on port X and transmitted on port Y or packets received on port Y and transmitted on port X.
- **XrxOrYtx**: Mirror packets received on port X or transmitted on port Y

MAC address-based modes

- **Asrc**: Mirror packets with source MAC address A.
- **Adst**: Mirror packets with destination MAC address A
- **AsrcOrAdst**: Mirror packets with source or destination MAC address A.
- **AsrcBdst**: Mirror packets with source MAC address A and destination MAC address B.
- **AsrcBdstOrBsrcAdst**: Mirror packets with source MAC address A and destination MAC address B or packets with source MAC address B and destination MAC address A.

Many-to-many port mirroring functionality

Many-to-Many Port Mirroring builds on the existing Port Mirroring application. Multiple instances are each configurable by using the existing interface. Each instance is attached to one Monitor Port (MTP). In some cases a monitor port can be used in more than one instance. Up to four instances are available.

The ports which are configured as MTP are not allowed to be part of a MLT group.

Many-to-many port mirroring restrictions

Many-to-Many Port Mirroring is only available on pure Ethernet Routing Switch 5600 Series stacks or stand-alone Ethernet Routing Switch 5600 Switches.

On startup, if a hybrid stack or standalone 5500 series unit is detected (stack oper-mode should be configured to hybrid), only the default instance is available and the user interface does not provide a way to configure another instance. An error message is returned if this is attempted.

If a 5500 series unit is inserted in a pure 5600 stack (stack oper-mode should be configured to hybrid), and multiple instances of Port Mirroring are configured on the stack, because the stack is now a hybrid one, only the default instance is kept active and the user interface changes such that

only this instance is applied and can be configured. If this is the case, the user can only use only this instance entirely. If all the 5500 series units are removed from a Stack (stack oper-mode should be changed to pure) all the enabled instances are re-applied.

In a hybrid stack if all 5500 series units are removed and only one 5600 series unit remains all port mirroring instances will become available. (the 5600 series unit remains in standalone mode and stack oper-mode has no sense in this case).

An MTP cannot be a mirrored port for another MTP. Frames mirrored to one MTP are not taken into account in MAC address-based mirroring on another MTP.

A port cannot be configured as MTP in an instance if it is already a mirrored port in another instance.

If a port is egress-mirrored in one instance, it cannot be egress-mirrored in another instance (to another MTP). The same applies to ingress-mirrored ports. A port can be ingress-mirrored in one instance and egress-mirrored in another.

The ports that are configured as MTP cannot participate in a normal frame switching operation.

Stack loopback tests

You can quickly test your stack ports and stack cable by using the stack loopback test. The stack loopback test is useful after you need to determine whether the source of the problem is a defective stack cable or a damaged stack port. The test can help prevent unnecessarily sending switches for service.

Two types of loopback tests exist. The internal loopback test verifies that the stack ports are functional.

The external loopback test checks the stack cable to determine if it is the source of the problem. Perform the external loopback test by connecting the stack uplink port with the stack downlink port, sending a packet from the uplink port, and verifying that the packet is received on the downlink port.

Always run the internal test first. Because the cable tests are not conclusive until you ensure the stack ports work correctly.

Stack monitor

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

The stack monitor sends a trap for the following events.

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

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

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

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

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 startup. The switch displays CPU utilization as a percentage. With CPU utilization information you can see how the CPU was used during a specific time interval.

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

No configuration is required for this display-only feature.

Light Emitting Diode display

The device displays diagnostic and operation information though the Light Emitting Diodes (LED) on the unit. Familiarize yourself with the interpretation of the LEDs on the Ethernet Routing Switch 5000 Series device. For information about the LED display see*Nortel Ethernet Routing Switch 5000 Series — Installation* (NN47200-300).

Power over Ethernet allocations

Devices such as IP phones, Web cameras, wireless access points that utilize Power over Ethernet (PoE). The switch displays the PoE allocations for each port. The PoE standard (802.3af) imposes the Power Devices (PD) that require power to run at 48 V and not draw more than 16 W.

The switch has multiple ports that are PoE capable. You must make consideration for the total power and maximum power provided required for each port and unit. Another important aspect is that of device priority. You must decide which device receives power when there is not enough for all.

Use the syslog to check the parameters. The following traps are logged:

- **pethPsePortOnOffNotification**: indicates if the switch port delivers power to the connected device. This notification is sent on every status change except in the search mode.
- **pethMainPowerUsageOnNotification**: indicates that the switch threshold usage indication is on and the usage power is higher than the threshold.
- **pethMainPowerUsageOffNotification** : indicates that the switch threshold usage indication is off and the usage power is lower than the threshold.

Displaying PoE allocations using NNCLI

Use this procedure to display the PoE status for the switch.

Procedure Steps

Step	Action
1	Use the **`show poe-main-status`** command to display the overall status of PoE.
2	Observe the NNCLI output.
3	Use the **`show poe-port-status`** command to display the port-level PoE status.
4	Observe the NNCLI output.

5 Use the **show poe-power-measurement** command to display power allocations on the switch.

6 Observe the NNCLI output.

--End--

Displaying PoE allocations using Web-based management

Use the Web-based management to display the PoE status for the switch. Use the dialogue boxes to configure and to observe current PoE status.

Step	Action
1	Navigate to **Configuration, PoE Management, Global Power Mgmt** to view overall PoE status on the switch.
2	Observe the information in the dialogue box.
3	Navigate to **Configuration, PoE Management, Port Property** to view port-level PoE information.
4	Observe the information in the dialogue box.

--End--

IP Flow Information Export

IP Flow Information Export (IPFIX) is a protocol used to export flow information from traffic observed on a switch. Because IPFIX is still in development with the IETF, the current implementation is based on Netflow Version 9.

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

- protocol type
- destination IP address
- source IP address.
- ingress port
- TOS

You can not use IPFIX on secondary interfaces.

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

- source port
- destination port

Release 5.0and later supports IPFIX through the creation and display of sampled information as well as the ability to export this sampled information. You can access IPFIX accessed through Device Manager or Web-based management.

The IPFIX feature shares resources with QoS. If the IPFIX feature is enabled, a QoS policy precedence is used. For further information about QoS policies, see the *Nortel Ethernet Routing Switch 5500 Series Configuration — Quality of Service* () (NN47200-504).

Remote Network Monitoring

The Remote Network Monitoring (RMON) MIB is an interface between the RMON agent on the Nortel Ethernet Routing Switch 5500 Series and an RMON management application, such as the Device Manager.

RMON defines objects that are suitable for managing any type of network, but some groups are targeted specifically for Ethernet networks.

The RMON agent continuously collects statistics and monitors switch performance.

RMON has three major functions:

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

Stack Health Check

The Stack Health Check feature provides information on the stacking state of each switch rear port. It is used to run a high-level test to monitor the rear port status for each unit, confirm the number of switching units in stack, detect if the stack runs with a temporary base unit, and to monitor stack continuity.

This feature is available through the NNCLI and Web-based management.

Displaying environmental information

This feature provides information on the status of the environment of each unit in a stack. It is used to perform the following tasks:

- Monitor the hardware status for each unit.
- Detect the presence of AC, DC, or AC/DC power.
- Monitor the CPUs temperature.
- Identify damaged or missing hardware.

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 Executive mode.
2	Enter the **show stack monitor** command.

--End--

Job Aid

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

```
5698TFD#show stack-monitor
Status:  disabled
Stack size:  2
Trap interval:  60
5698TFD#
```

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--

Table 3
Variable Definitions

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--

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
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	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 Executive 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:

```
5698TFD#stack loopback-test internal
Testing uplink port ... ok

Testing downlink port ... ok
Internal loopback test PASSED.
5698TFD#
```

```
5698TFD#stack loopback-test external
External loopback test PASSED.
5698TFD#
```

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

```
5698TFD#stack loopback-test internal
Testing uplink port ... Failed
Testing downlink port ... ok
Internal loopback test FAILED.
5698TFD#
```

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:

```
5698TFD#stack loopback-test external
External loopback test FAILED. Your stack cable might be
damaged.
5698TFD#
```

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

```
5698TFD#stack loopback-test internal
Stack loopback test affects the functioning of the stack.
You should run this in stand-alone mode
5698TFD#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 Executive 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 5000 series unit and on port 2 on another 5000 series 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

Perform this procedure to display port configuration information.

Procedure Steps

Step	Action
1	Enter Privileged Executive 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.

```
5698TFD#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 4
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 5
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 6
Spanning-tree port configurations

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

Showing stack health information

Perform this procedure to display stack health information.

Procedure 1
Procedure steps

Step	Action
1	Enter Privileged Executive mode
2	Enter the **show stack health** command.
3	Observe the NNCLI output.

--End--

Job aid

The following is an example of the **show stack health** command output when the stack is formed but did not end the initialization process.

```
#show stack health
Stack in progress
```

The following is an example of the **show stack health** command output when the stack is formed and initialized, and all the rear ports are up.

```
#show stack health
-----------------------------------------------------------------
-
Unit# Switch Model Cascade Up Cascade Down
-----------------------------------------------------------------
--
1 (Base) 5698TFD-PWR OK OK
2 5650TD OK OK
3 5520-48T-PWR OK OK
4 5510-24T OK OK
5 5510-48T OK OK
6 5698TFD OK OK
7 5510-24T OK OK
-----------------------------------------------------------------
--
Switch Units Found = 8
Stack Health Check = OK - RESILIENT
Stack Diagnosis = Stack in full resilient mode
```

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

```
#show stack health
```

```
-------------------------------------------------------------
-
Unit# Switch Model Cascade Up Cascade Down
-------------------------------------------------------------
--
1 (Base) 5698TFD-PWR OK OK
2 5650TD OK OK
3 5520-48T-PWR OK OK
4 5510-24T OK LINK DOWN OR MISSING
6 5510-48T LINK DOWN OR MISSING OK
7 5698TFD OK OK
8 5510-24T OK OK
-------------------------------------------------------------
--
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).
```

The following 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.

```
#show stack health
-------------------------------------------------------------
-
Unit# Switch Model Cascade Up Cascade Down
-------------------------------------------------------------
--
1 (Base) 5698TFD-PWR OK OK
2 5650TD OK OK
3 5520-48T-PWR OK OK
4 5510-24T OK OK
5 5510-24T OK OK
6 5510-48T OK UP WITH ERRORS
7 5698TFD UP WITH ERRORS OK
8 5510-24T OK OK
-------------------------------------------------------------
--
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).
```

A cable is not considered problematic (`UP WITH ERRORS`) when the switch connected to the other side is up but not in stack, or when the switch connected to the other side is up and in stack. A cable is considered problematic after several changes of status (between `OK` and `LINK DOWN`) occur in a short amount of time.

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

```
#show stack health
-----------------------------------------------------------
-
Unit# Switch Model Cascade Up Cascade Down
-----------------------------------------------------------
--
1 5698TFD-PWR OK OK
2 (Temporary Base) 5650TD OK OK
3 5520-48T-PWR OK OK
4 5510-24T OK OK
5 5510-24T OK OK
6 5510-48T OK OK
7 5698TFD OK OK
8 5510-24T OK OK
-----------------------------------------------------------
--
Switch Units Found = 8
Stack Health Check = OK - RESILIENT
Stack Diagnosis = Stack in full resilient mode.
```

The following is an example of the **show stack health** command output when the stack is formed and initialized and there are damaged or missing rear links and a temporary base unit.

```
#show stack health
-----------------------------------------------------------
-
Unit# Switch Model Cascade Up Cascade Down
-----------------------------------------------------------
--
2(Temporary Base) 5698TFD-PWR LINK DOWN OR MISSING OK
3 5650TD OK OK
4 5520-48T-PWR OK OK
5 5510-24T OK OK
6 5510-24T OK OK
7 5510-48T OK OK
8 5698TFD OK LINK DOWN OR MISSING
-----------------------------------------------------------
--
Switch Units Found = 7
Stack Health Check = WARNING - NON-RESILIENT WITH TEMPORARY BASE
Stack Diagnosis = Stack in non-resilient mode, with temporary
base unit.
Recommend replacing failed base unit or to add/replace the
identified cables.
```

Job aid

Perform this procedure to ensure that the stack has the correct number of switching units and that it is running in resilient mode. If the stack is not running in resilient mode, use this procedure to identify damaged or missing cables and to repair faulty stacks.

Procedure 2
Procedure steps

Step	Action
1	Display the stack health status from the NNCLI.
2	If the number of units is the same as expected and the stack is resilient, this procedure is complete.
3	If the number of units is the same as expected, but the stack is not resilient, add or replace the identified cables and repeat the entire procedure.
4	If the number of units is not the same as expected, ensure all switching units are present and running and that they are properly connected.
5	If all the units are operational, but the number of units is not properly shown, remove or replace the units that do not appear.

--End--

Viewing environmental information

Perform this procedure to view the status of the unit or stack environment.

Procedure steps

Step	Action
1	Enter Privileged Executive mode
2	Enter the **`show environmental`** command.
3	Observe the NNCLI output.

--End--

Job aid

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

```
5698TFD-PWR#show environmental
Unit #1
```

```
Power Supply 1:  AC-DC-12V-300W
Power Supply 2:  Unavailable
Power Supply 3:  Unavailable
Fan #1:  OK
Fan #2:  OK
Fan #3:  OK
Fan #4:  OK
Fan #5:  OK
Fan #6:  OK
Temperature:  OK 36C
Unit #2
Power Supply 1:  Unavailable
Power Supply 2:  Unavailable
Power Supply 3:  AC-DC-48V-100W
Fan #1:  OK
Fan #2:  OK
Fan #3:  OK
Fan #4:  OK
Fan #5:  OK
Fan #6:  OK
Temperature:  OK 37C
```

Job aid

Perform this procedure to ensure that the unit or stack works in proper conditions.

Procedure steps

Step	Action
1	Display the unit or stack environmental information from the NNCLI.
2	If the information that appears indicates that each unit hardware environment is in good condition you have completed this procedure.
3	If the temperature is High or the fans have a Fail status,check the hardware.
4	Execute hardware maintenance.
5	Repeat steps 1 to 5 if necessary.

--End--

System diagnostics and statistics using Web-based management

This chapter contains information regarding using Web-based management for system diagnostics and statistics.

Navigation

Viewing port statistics using Web-based management

View statistical data about a selected port.

Procedure Steps

Step	Action
1	To open the **Port Statistics** window, select **Statistics, Port** from the menu.
2	Select a port from the **Port** list in the **Port Statistics (View By)** section.
3	Click **Update** to refresh the statistical information.
4	Click **Zero Port** to reset the counters for the selected port.

5 Click **Zero All Ports** to reset the counters for all ports.

6 Click **Submit**.

--End--

Job Aid

Port statistics are displayed in the **Port Statistics Table** section. The following table describes the fields in this section.

Table 7
Port Statistics Table fields

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).
Oversized Packets	The number of packets that were 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 were 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 that counter. This 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.

Field	Description
Collisions	The number of collisions detected on this port.
Single Collisions	The number of packets that were transmitted successfully on this port after a single collision.
Multiple Collisions	The number of packets that were 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 were received on this port that were 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 1522-9216 bytes	The number of packets received/transmitted on the port.

Viewing all port errors

To view a summary of the port errors, follow this procedure:

Step	Action
1	Open the **Port Error Summary** window by selecting **Statistics, Port Error Summary** from the menu.
2	Click **Update** to refresh the statistical information.

--End--

Job Aid

The following table describes the fields on the Port Error Summary window.

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).

Field	Description
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.

Displaying port-mirroring using Web-based management

Web-based management displays all instances of port-mirroring.

Step	Action
1	Navigate to **Application, Port Mirroring**
2	Observe the modes and the instances displayed.

--End--

Job Aid

The following table describes the fields in the display area of the port mirroring window.

Field	Description
Monitor Mode	The monitoring mode for the instance.
Monitor Port	The monitor port that is configured for the instance.
Port X	The port being monitored

Configuring port-mirroring using Web-based management

With Web-based management you can configure the instances of port-mirroring.

Step	Action
1	Navigate to **Application, Port Mirroring**
2	Input the instance number to be modified in the **Instance** field.
3	Select the monitoring mode in the **Monitoring Mode** field.
4	Select the monitor port in the **Monitor Port** field.
5	Select the receiving port from in the **Port X** field.
6	If applicable, select the transmitting port from in the **Port Y** field.
7	Click the **Submit** button.

--End--

Job Aid

The following table describes the fields in the display area of the port mirroring window.

Field	Description
Instance	The instance being configured.
Monitoring mode	The mode for the instance.
Monitor Port	The port configured as the monitor port.
Port X	The monitored port that has the packets transmitted.
Port Y	The monitored port that has the packets received.

Viewing interface statistics

To view statistical information for an interface, follow this procedure:

Step	Action
1	Open the **Interface Statistics** window by selecting **Statistics, Interface** from the menu. This window is illustrated in the following table.
2	Click **Update** to refresh the statistical information.

--End--

Job Aid

The following table describes the fields on this window.

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 be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
In Non-Unicast	The number of non-unicast 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 be transmitted to a non-unicast address. For example, a subnetwork-broadcast or a subnetwork multicast address, including those that were discarded or not sent.
In Discards	The number of inbound packets which were selected to be discarded even though no errors were 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 which were selected to be discarded even though no errors were detected to prevent their being transmitted. Packet discarding is not arbitrary. One reason for discarding packets is to free 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 could not be transmitted because of errors.
In Unknown Protos	The number of packets received through the interface that were discarded because of an unknown or unsupported protocol.

Viewing Ethernet error statistics

To view Ethernet error statistics, follow this procedure:

Step	Action
1	Open the **Ethernet Errors** window by selecting **Statistics, Ethernet Errors** from the menu. This window is illustrated in the following table.
2	Select **Update** to refresh the statistical information.

--End--

Job Aid

The following table outlines the fields on this window.

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 was lost or never asserted after 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.

Field	Description
Single Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
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.

Viewing transparent bridging statistics

To view transparent bridging statistics, follow this procedure:

Step	Action
1	Open the **Transparent Bridging** window by selecting **Statistics, Transparent Bridging** from the menu.
2	Click **Update** to refresh the statistical information.

--End--

Job Aid

The following table describes the fields on the Transparent Bridging window.

Field	Description
Port	The port number that corresponds to the selected switch.
In Frames (dot1dTpPortInFrames)	The number of frames that have been 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 that have been transmitted 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.
In Discards (dot1dTpPortInDiscards)	The number of valid frames received which were discarded by the forwarding process.

Monitoring MLT traffic

Bandwidth usage can be monitored for the Multilink Trunk (MLT) member ports within each trunk in a configuration by selecting the traffic type to monitor.

To monitor MultiLink Trunk traffic, follow this procedure:

Step	Action
1	Open the **MLT Utilization** window by selecting **Application, MultiLink Trunk, Utilization** from the menu.
2	In the **MultiLink Trunk Utilization Selection (View By)** section, select a trunk to monitor in the **Trunk** list and a type of traffic in the **Traffic Type** list.
3	Click **Submit**.

--End--

Job Aid

The following table describes the fields in this table.

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.

Viewing stack health

Perform this procedure to display stack health information.

Procedure steps

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

--End--

Job aid

Perform this procedure to ensure that the stack has the correct number of switching units and that it is running in a resilient mode. If the stack is not running in a resilient mode, perform this procedure to identify damaged or missing cables, and to repair faulty stacks.

Procedure steps

Step	Action
1	Display the stack health status from Web-based management.
2	If the number of units is the same as expected, and the stack is resilient, this procedure is complete.
3	If the number of units is the same as expected, but the stack is not resilient, add or replace the identified cables and repeat the entire procedure.
4	If the number of units is not the same as expected, ensure all switching units are present and running and that they are properly connected.
5	If all units are operational, but the number of units is not properly shown, remove or replace the units that do not appear.

--End--

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 Stack Monitor with Device Manager" (page 55)

Configuring Stack Monitor with Device Manager

Use the DM to configure the Stack Monitor.

Procedure Steps

Step	Action
1	Select the chassis.
2	From the 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--

Network monitoring configuration using NNCLI

This chapter describes using NNCLI to view and configure network monitoring.

Navigation

Viewing CPU utilization

Use this procedure to view the CPU utilization

Viewing CPU utilization using NNCLI

Step	Action
1	Enter Privileged Executive mode.
2	Enter the **`show cpu-utilization`** command.
3	Observe the displayed information.

--End--

Viewing memory utilization

Use this procedure to view the memory utilization

Viewing memory utilization using NNCLI

Step	Action
1	Enter Privileged Executive mode.
2	Enter the **show memory-utilization** command.
3	Observe the displayed information.

--End--

Configuring the system log

This section outlines the NNCLI commands used in the configuration and management of the system log.

Displaying the system log

Use this procedure to displays the configuration, and the current contents, of the system event log.

Procedure Steps

Step	Action
1	Enter the **show show logging [config] [critical] [serious] [informational] [sort-reverse]** command Privileged Executive mode.

--End--

Variable definitions

The following table describes the command variables.

Variable	Value
config	Display 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).

Configuring the system log

Use this procedure to configure the system settings for the system event log.

Procedure Steps

Step	Action
1	Enter the **logging [enable | disable] [level critical | serious | informational | none] [nv-level critical | serious | none]** command Privileged Executive mode.

--End--

Variable definitions

The following table describes the command variables.

Variable	Value
enable | disable	Enables or disables the event log (default is Enabled).
level critical | serious | informational | none	Specifies the level of logging stored in DRAM.
nv-level critical | serious | none	Specifies the level of logging stored in NVRAM.

Disabling the system log

Use this procedure to disable the system event log.

Procedure Steps

Step	Action
1	Enter the **no logging** command in global configuration mode.

--End--

Setting the system log to default

Use this procedure to default the system event log configuration.

Procedure Steps

Step	Action
1	Enter the **`default logging`** command in global configuration mode.

--End--

Clearing the system log

Use this procedure to clear all log messages in DRAM.

Procedure Steps

Step	Action
1	Enter the **`clear logging [non-volatile] [nv] [volatile]`** command in global configuration mode.

--End--

Variable definitions

The following table describes the command variables.

Table 8
clear logging parameters

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

Configuring remote logging

Use the NNCLI to configure remote logging. This section discusses the commands that enable remote logging.

Displaying logging

Use this procedure to display the configuration and the current contents of the system event log.

Procedure steps

Step	Action
1	Enter Global Configuration mode.

2 Enter the **show logging** command to display the log.

--End--

Enabling remote logging

Use this procedure to enable remote logging. By default, remote logging is disabled.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **logging remote enable** command to enable the use of a remote syslog server.

--End--

Disabling remote logging

Use this procedure to disable remote logging.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **no logging remote enable** command to disable the use of a remote syslog server.

--End--

Setting the remote logging address

Use this procedure to set the address of the remote server for the syslog.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **logging remote address <A.B.C.D>** command to disable the use of a remote syslog server.

--End--

Variable Definitions

The following table describes the command variables.

Parameters and variables	Description
<A.B.C.D>	Specifies the IP address of the remote server in dotted-decimal notation. The default address is 0.0.0.0.

Clearing the remote server IP address

Use this procedure to clear the IP address of the remote server.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **no logging remote address** command to clear the IP address of the remote syslog server.

--End--

Setting the log severity

Use this command to set the severity level of the logs sent to the remote server.

Procedure

Step	Action
1	Enter Global Configuration mode.
2	Enter the **logging remote level {critical | informational | serious | none}** command to set the severity level of the logs that will be sent to the server.

--End--

Variable definitions

The following table describes the command variables.

Parameters and variables	Description
{critical | serious | informational | none}	Specifies the severity level of the log messages to be sent to the remote server: • critical • informational • serious • none

Resetting the severity level

Use this command to remove severity level setting

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **`no logging remote level`** command to remove the severity level of the logs that will be sent to the server. The level is set to none.

--End--

Setting the default remote logging level

Use this procedure to set the remote logging level to default.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **`default logging remote level`** command to sets the severity level of the logs sent to the remote server. The default level is none.

--End--

Configuring port mirroring

Port mirroring can be configured with the NNCLI commands detailed in this section.

Displaying the port-mirroring configuration

Use this procedure to display the existing port-mirroring configuration.

Procedure Steps

Step	Action
1	Enter Privileged Executive mode.
2	Enter the **show port-mirroring** command to display the port-mirroring configuration.

--End--

Configure port-mirroring

Use this procedure to set the port-mirroring configuration

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **port-mirroring mode {disable | Xrx monitor-port <portlist> mirror-ports <portlist> | Xtx monitor-port <portlist> mirror-ports <portlist> | ManytoOneRx monitor-port <portlist> mirror-ports <portlist> | ManytoOneTx monitor-port <portlist> mirror-port-X <portlist> | ManytoOneRxTx monitor-port <portlist> mirror-port-X <portlist> | XrxOrXtx monitor-port <portlist> mirror-port-X <portlist> | XrxOrYtx monitor-port <portlist> mirror-port-X <portlist> mirror-port-Y <portlist> | XrxYtxmonitor-port <portlist> mirror-port-X <portlist> mirror-port-Y <portlist> | XrxYtxOrYrxXtx monitor-port <portlist> mirror-port-X <portlist> mirror-port-Y <portlist> | Asrc monitor-port <portlist> mirror-MAC-A <macaddr> | Adst monitor-port <portlist> mirror-MAC-A <macaddr> | AsrcOrAdst monitor-port <portlist> mirror-MAC-A <macaddr> | AsrcBdst monitor-port <portlist> mirror-MAC-A <macaddr> mirror-MAC-B <macaddr> | AsrcBdstOrBsrcAdst monitor-port <portlist> mirror-MAC-A <macaddr> mirror-MAC-B <macaddr>}** command to display the port-mirroring configuration.

--End--

Variable definitions

The following table outlines the parameters for this command.

Parameter	Description
disable	Disables port-mirroring.
monitor-port	Specifies the monitor port.
mirror-port-X	Specifies the mirroring port X.
mirror-port-Y	Specifies the mirroring port Y.
mirror-MAC-A	Specifies the mirroring MAC address A.
mirror-MAC-B	Specifies the mirroring MAC address B.
portlist	Enter the port numbers.
ManytoOneRx	Many to one port mirroring on ingress packets.
ManytoOneTx	Many to one port mirroring on egress packets.
ManytoOneRxTx	Many to one port mirroring on ingress and egress traffic.
Xrx	Mirror packets received on port X.
Xtx	Mirror packets transmitted on port X.
XrxOrXtx	Mirror packets received or transmitted on port X.
XrxYtx	Mirror packets received on port X and transmitted on port Y. This mode is not recommended for mirroring broadcast and multicast traffic.
XrxYtxOrXtxYrx	Mirror packets received on port X and transmitted on port Y or packets received on port Y and transmitted on port X.
XrxOrYtx	Mirror packets received on port X or transmitted on port Y.
macaddr	Enter the MAC address in format H.H.H.
Asrc	Mirror packets with source MAC address A.
Adst	Mirror packets with destination MAC address A.
AsrcOrAdst	Mirror packets with source or destination MAC address A.
AsrcBdst	Mirror packets with source MAC address A and destination MAC address B.
AsrcBdstOrBsrcAdst	Mirror packets with source MAC address A and destination MAC address B or packets with source MAC address B and destination MAC address A.

Disabling port-mirroring

Use this procedure to disable port-mirroring

Procedure Steps

Step	Action
1	Enter Global Configuration mode
2	Enter the **no port-mirroring** command to disable port-mirroring.

--End--

Displaying Many-to-Many port-mirroring

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

Procedure Steps

Step	Action
1	Enter Privileged Executive mode
2	Enter the **show port-mirroring** command.
3	Observe the displayed information.

--End--

Configuring Many-to-Many port-mirroring

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

Procedure Steps

Step	Action
1	Enter Global Configuration mode
2	Enter the **port-mirroring <1-4> mode {disable | Adst | Asrc | AsrcBdst | AsrcBdstOrBsrcAdst | AsrcOrAdst | ManyToOneRx | ManyToOneRxTx | ManyToOneTx | Xrx | XrxOrXtx | XrxOrYtx | XrxYtx | XrxYtxOrYrxXtx | Xtx}** command.
3	Enter the command from step 2 for up to four instances.

--End--

Variable definitions

The following table describes the command variables

Variable	Value
disable	Disable mirroring.
Adst	Mirror packets with destination MAC address A
Asrc	Mirror packets with source MAC address A.
AsrcBdst	Mirror packets with source MAC address A and destination MAC address B.
AsrcBdstOrBsrcAdst	Mirror packets with source MAC address A and destination MAC address B or packets with source MAC address B and destination MAC address A.
AsrcOrAdst	Mirror packets with source or destination MAC address A.
ManyToOneRx	Mirror many to one port mirroring on ingress packets.
ManyToOneRxTx	Mirror many to one port mirroring on ingress and egress packets.
ManyToOneTx	Mirror many to one port mirroring on egress packets.
Xrx	Mirror packets received on port X.
XrxOrXtx	Mirror packets received on port X and transmitted on port Y.
XrxYtx	Mirror packets received on port X and transmitted on port Y.
XrxYtxOrYrxXtx	Mirror packets received on port X and transmitted on port Y or packets received on port Y and transmitted on port X.
Xtx	Mirror packets received on port X or transmitted on port Y

Disabling Many-to-Many port-mirroring

Procedure Steps

Step	Action
1	Enter Global Configuration mode
2	Enter the **`port-mirroring [<1-4>] mode disable`** or **`no port-mirroring [<1-4>]`** command to disable a specific instance.

3 Enter the **no port-mirroring** command to disable all instances.

--End--

Variable definitions

The following paragraph describes the command variables.

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

Network monitoring configuration using Device Manager

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.
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	Memory usage in megabytes.

Field	Description
MemoryTotalMB	Total memory present, in megabytes, on the unit.
MemoryAvailableMB	Memory remaining available on the unit.

Configuring the system log with Device Manager

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

Procedure 3
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.
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

Several screens in the Device Manager (DM) provide a means to view and make use of statistical information gathered by the switch. To turn this statistical information in either a bar, line, area, or pie graph, follow this procedure:

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

--End--

Graphing switch chassis data

The DM provides the ability to view switch statistical information in a variety of graphs.

To make use of these capabilities, open the **Graph Chassis** window by selecting **Graph, Chassis** from the menu.

The following sections describe the informational tabs on this window and the type of data each represents. Refer to “Creating a graph” (page 71) for the procedure to graph this data.

Viewing the SNMP tab

The **SNMP** tab provides read-only statistical information about SNMP traffic.

Use this procedure to view the **SNMP** tab.

Procedure Steps

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

2 Select the **SNMP** tab the **Graph Chassis** window.

--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.

Field	Description
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 after 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. This error 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

Use this procedure to view read-only information about the IP packets that are interfaced with the switch

Procedure Steps

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

2 Select the **IP** tab.

--End--

Job aid

The following table outlines the fields on this tab.

Table 9
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, errors discovered in processing their IP options.
InAddrErrors	The number of input datagrams discarded because the IP address in the IP header destination field was not a valid address. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For addresses that are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. For addresses that do not act as IP Gateways, this counter includes only those packets that were Source-Routed by way of this address and had successful Source-Route option processing.
InUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing but that were discarded (for example, for lack of buffer space). This counter does not include any datagrams discarded while awaiting reassembly.
InDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	The total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in ipForwDatagrams.

Field	Description
OutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that were discarded (for example, for lack of buffer space). This counter will include 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 have been successfully fragmented at this entity.
FragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, for example, because their Don't Fragment flag was set.
FragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
ReasmReqds	The number of IP fragments received that needed to be reassembled at this entity.
ReasmOKs	The number of IP datagrams successfully reassembled.
ReasmFails	The number of failures detected by the IP reassembly algorithm. 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

Use this procedure to view read-only information about inbound ICMP messages.

Procedure Steps

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

--End--

Job Aid

The following table describes the fields on this 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

Use this procedure to view read-only information about outbound ICMP messages.

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 fields on this 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 will always be 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.

Field	Description
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

Use this procedure to view read-only information about TCP activity on the switch.

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 this 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.

Field	Description
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

Use this procedure to view 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 appears.
2	Select the **UDP** tab.

--End--

Job Aid

The following table describes the fields on this tab.

Table 10
UDP tab fields

Field	Description
InDatagrams	The total number of UDP datagrams delivered to UDP users
NoPorts	The total number of received UDP datagrams for which there was no application at the destination port.
InErrors	The number of received UDP datagrams that could not 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.

Field	Description
HCInDatagrams	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
HCOutDatagrams	The number of UDP datagrams sent from this entity, for devices that can transmit more than 1 million UDP datagrams for each second. Discontinuities in the value of this counter can occur at reinitialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime.

Viewing the OSPF tab

Use this procedure to view statistical information about OSPF operation on the switch.

Procedure Steps

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

--End--

Job aid

The following table describes the fields on this tab.

Field	Description
LsdbTblSize	Indicates the number of entries in the link state database.
TxPackets	Indicates the number of packets transmitted by OSPF.
RxPackets	Indicates the number of packets received by OSPF.
RxBadPackets	Indicates the number of bad packets received by OSPF.
SpfRuns	Indicates the total number of SPF calculations performed by OSPF.
BuffersAllocated	Indicates the total number of buffers allocated by OSPF.
BuffersFreed	Indicates the total number of buffers freed by OSPF.
BufferAllocFailures	Indicates the number of times that OSPF has failed to allocate buffers.
BufferFreeFailures	Indicates the number of times that OSPF has failed to free buffers.

Viewing the VRRP tab

Use this procedure to view statistical information about VRRP operation on the switch.

Procedure Steps

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

--End--

Job aid

The following table describes the fields on this tab.

Field	Description
RouterChecksumErrors	The total number of VRRP packets received with an invalid VRRP checksum value.
RouterVersionErrors	The total number of VRRP packets received with an unknown or unsupported version number.
RouterVrIdErrors	The total number of VRRP packets received with an invalid VRID for this virtual router."

Graphing switch port data

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

Use the following procedure to select a port or ports to graph.

Procedure Steps

Step	Action
1	Select one or multiple ports on the device view.
2	Select **Graph, Port** from the menu.

--End--

The following sections describe the informational tabs on this window and what type of data each represents. Refer to “Creating a graph” (page 71) for the procedure to graph this data.

Some statistics are only available after a single port is graphed.

Viewing the Interface tab

Use this procedure to view read-only information about the selected interfaces.

Procedure Steps

Step	Action
1	Select one or multiple ports on the device view.
2	Select **Graph, Port** from the menu.
3	Select the **Interface** tab.

--End--

Job aid

The following table describes the fields on this tab.

Table 11
Interface tab fields

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 were not addressed to a multicast or broadcast address at this sublayer.
OutUcastPkts	The number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast address at this sublayer. This total number includes those packets discarded or unsent.
InNUcastPkts	The number of packets delivered by this sublayer to a higher (sub)layer, which were addressed to a multicast or broadcast address at this sublayer.
OutNUcastPkts	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent.
InDiscards	The number of inbound packets that were 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.

Field	Description
OutDiscards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet is to free up buffer space.
InErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
OutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.
InUnknownProtos	For packet-oriented interfaces, the number of packets received through the interface that were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received through the interface that were discarded because of an unknown or unsupported protocol. For an interface that does not support protocol multiplexing, this counter will always be 0.

Viewing Ethernet Errors tab

Use the following procedure to view read-only information about port Ethernet error statistics.

Procedure Steps

Step	Action
1	Select one or multiple ports on the device view.
2	Select **Graph, Port** from the menu.
3	Select the **Ethernet Errors** tab.

--End--

Job Aid

The following table describes the fields on this tab.

Table 12
Ethernet Errors tab fields

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 after 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 after 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 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 was lost or never asserted after 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 after 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

Use the following procedure to view read-only information about port frame statistics.

Procedure Steps

Step	Action
1	Select one or multiple ports on the device view.
2	Select **Graph, Port** from the menu.
3	Select the **Bridge** tab.

--End--

Job aid

The following table describes the fields on this tab.

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

Viewing the Rmon tab

Use the following procedure to view read-only remote monitoring statistics.

Procedure Steps

Step	Action
1	Select one or multiple ports on the device view.
2	Select **Graph, Port** from the menu.
3	Select the **Rmon** tab.

--End--

Job aid

The following table describes the fields on this tab.

Table 13
RMON tab fields

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 were directed to the broadcast address. This does not include multicast packets.
MulticastPkts	The total number of good packets received that were 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 were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
OversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.

Field	Description
Fragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Normal behavior is for etherStatsFragments is 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 were 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 a packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
1..64	The total number of packets (including bad packets) received that were 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 that were 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 that were 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 that were 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 that were 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 that were between 1024 and 1518 octets in length (excluding framing bits but including FCS octets).

Viewing the EAPOL Stats tab

Use the following procedure to view read-only EAPOL statistics.

Procedure Steps

Step	Action
1	Select one or multiple ports on the device view.
2	Select **Graph, Port** from the menu.

3 Select the **EAPOL Stats** tab.

--End--

Job aid

The following table describes the fields on this tab.

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

Viewing the EAPOL Diag tab

Use the following procedure to view read-only EAPOL diagnostic statistics.

Procedure Steps

Step	Action
1	Select one or multiple ports on the device view.
2	Select **Graph, Port** from the menu.

3 Select the **EAPOL Diag** tab.

--End--

Job aid

The following table describes the fields on this tab.

Table 14
EAPOL Diag tab fields

Field	Description
EntersConnecting	Counts the number of times that the Authenticator PAE state machine transitions to the Connecting state from another 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.

Field	Description
AuthTimeoutsWhileAuthenticating	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.
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.

Field	Description
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

Use the following procedure to view read-only Link Aggregation Control Protocol (LACP) diagnostic statistics.

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

Procedure Steps

Step	Action
1	Select one or multiple ports on the device view.
2	Select **Graph, Port** from the menu.
3	Select the **LACP** tab.

--End--

Job aid

The following table describes the fields on this tab.

Table 15
LACP tab fields

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.

Field	Description
MarkerResponsePDUsRX	The number of valid Marker Response PDUs received on this Aggregation Port. This value is read-only.
UnknownRX	Indicates the number of frames received that can • 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 that are transmitted on this Aggregation Port. This value is read-only.
MarkerPDUsTX	Displays the number of Marker PDUs transmitted on this Aggregation Port. This value is read-only.
MarkerResponsePDUsTX	Indicates the number of Marker Response PDUs that are transmitted on this Aggregation Port. This value is read-only.

Viewing the Misc tab

Use the following procedure to view statistical information that does not belong grouped with the other tabs.

Procedure Steps

Step	Action
1	Select one or multiple ports on the device view.
2	Select **Graph, Port** from the menu.
3	Select the **Misc** tab.

--End--

Job aid

The following table describes the fields on this tab.

Table 16
Misc tab fields

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

Graphing multilink trunk statistics

This section describes using Device Manager (DM) provides to view Multilink Trunk (MLT) statistical information in a variety of graphs.

Use the following procedure to access the MLT statistics window.

Procedure Steps

Step	Action
1	Select **VLAN, MLT/LACP** from the menu.
2	Select the Multilink Trunks tab.
3	Select the row that represents the MLT and select the **Graph** button.

--End--

To make use of these capabilities, open the **MLT_LACP** window by This window opens with the **Multilink Trunks** tab selected. On this tab, select the row that represents the **MLT** to graph and click the **Graph** button. The **MLT Statistics** window appears.

Viewing the Interface tab

Use the following procedure to view read-only statistical information about the selected Multilink Trunk.

Step	Action
1	Select **VLAN, MLT/LACP** from the menu.
2	Select the Multilink Trunks tab.
3	Select the row that represents the MLT and select the **Graph** button.
4	Select the **Interface** tab.

--End--

Job aid

The following table describes the fields on this tab.

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

Viewing the Ethernet Errors tab

Use the following procedure to view read-only statistical information about Ethernet errors that have occurred on the selected Multilink Trunk.

Step	Action
1	Select **VLAN, MLT/LACP** from the menu.
2	Select the Multilink Trunks tab.
3	Select the row that represents the MLT and select the **Graph** button.
4	Select the **Ethernet Errors** tab.

--End--

Job aid

The following table describes the fields on this 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 after 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 after 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.

Field	Description
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.
CarrierSenseErrors	The number of times that the carrier sense condition was lost or never asserted after attempting to transmit a frame on a particular MLT. The count represented by an instance of this object is incriminated 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 after 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.

Field	Description
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.
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.

Graphing VLAN DHCP statistics

Use the following procedure to create a graph of VLAN DHCP configuration.

Procedure Steps

Step	Action
1	Open the VLANs window by selecting **VLAN, VLANs** from the menu.
2	Select the desired VLAN.
3	Click **IP**. The IP VLAN window opens with the IP Address tab selected.
4	Click the **DHCP** tab.
5	Click **Graph**. The DHCP Stats window appears.
6	Highlight the required data and click on the type of graph to produce. For a detailed explanation of graph creation

--End--

Job aid

The following table explains the fields found on this window.

Field	Description
NumRequests	The number of DHCP requests handled.
NumReplies	The number of DHCP replies handled.

Viewing unit statistics

Use this procedure to view the statistical information of a unit.

Procedure 4
Procedure steps

Step	Action
1	Select a unit on the device view.
2	Select **Edit > Unit** from the menu.
3	Select the **Unit Stats** tab.

--End--

Job aid

The following table describes the fields in this tab.

Field	Description
Absolute Value	The counter value of packets dropped for the unit.
Cumulative	The total value of packets dropped seen since dialog displayed.
Average/sec	The average value of packets dropped per second.
Minimum/sec	The smallest value of packets dropped seen per second.
Maximum/sec	The largest value of packets dropped seen per second.
LastVal/sec	The last value of packets dropped seen per second.

Network monitoring configuration using Web-based management

Viewing CPU and memory utilization

Use this procedure to display both CPU and memory utilization.

Procedure Steps

Step	Action
1	Open Web-based management
2	Navigate to **Administration, CPU / Memory Utilization**
3	Observe the displayed CPU and memory utilization in the window.

--End--

Job aid

The following table describes the fields in the window.

Field	Description
From System Boot-Up	CPU utilization since system boot-up
Last 10 Seconds	CPU utilization for the last 10 seconds
Last 1 Minute	CPU utilization for the last minute
Last 10 Minutes	CPU utilization for the last 10 minutes
Last 60 Minutes	CPU utilization for the last 60 minutes
Last 24 Hours	CPU utilization for the last 24 hours
Total	Total memory in the device
Used	Amount of memory in use
Free	Amount of memory available

Viewing the system log in the Web-based management

Use the following procedure 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 to be displayed by selecting a value from the **Display Messages From** list.
3	Click **Submit**.

--End--

Clearing system log messages using Web-based management

Use the following procedure to clear system log messages.

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 to be displayed by selecting a value from the **Clear Messages From** list.
3	Click **Submit**.

--End--

Configuring port mirroring with the Web-based management

Use the following procedure to configure port-mirroring.

Procedure Steps

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 outlines the fields in this section.

3 Click **Submit**.

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

--End--

Job Aid

The following table describes the fields in this window.

Field	Description
Monitoring Mode	Choose one of the six port-based monitoring modes or one of the nine 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 <->\n• ManyToOneRx • ManyToOneTx • ManyToOneRxTx • 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 will act as the monitoring port.
Port X	In port-based configurations, choose the first switch port to be monitored by the designated monitor port. This port is monitored according to the value "X" in the Monitoring Mode field.
Port Y	In port-based configurations, choose the second switch port to be monitored by the designated monitor port. This port is monitored according to the value "Y" in the Monitoring Mode field.

Field	Description
Address A	In address-based configurations, type the MAC address to monitor by the designated monitor port. This address is monitored according to the value "Address A" in the Monitoring Mode field.
Address B	In address-based configurations, type the MAC address to monitor by the designated monitor port. This address is monitored according to the value "Address B" in the Monitoring Mode field.

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

Use the following procedure to retrieve the value of a SNMP object by name or OID.

Step	Action
1	Navigate to the **Administration, Mib Web Page** window.
2	Enter the object name or OID in the **SNMP Object Name/ OID** field.
3	Click the **Get** button.
4	Observe the information displayed in the **Result** area of the window.
5	Click the **Get Next** button to retrieve the information of the next object in the MIB.
6	Observe the information displayed in the **Result** area of the window. Repeat this step for as long as required.

--End--

Using the MIB Web page for SNMP walk

Use the following procedure to retrieve the value of a SNMP object by name or OID.

Step	Action
1	Navigate to the **Administration, SNMP Mib Walk** window.
2	Enter the object name or OID in the **SNMP Object Name/ OID** field.
3	Click the **Walk** button.
4	Observe the information displayed in the **Result** area of the window.

5 Click **Next** or **Previous** to view the next or previous twelve objects in the MIB.

--End--

Using the trap Web page to identify trap receivers

Use the following procedure to identify the trap receivers.

Configuring traps using the Trap Web Page

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

--End--

RMON configuration using NNCLI

Configuring RMON with the NNCLI

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

Viewing RMON alarms

Use the following procedure to view RMON alarms.

Procedure Steps

Step	Action
1	Enter Privileged Executive mode.
2	Use the **show rmon alarm** command to display information about RMON alarms.

--End--

Viewing RMON events

Use the following procedure to display information regarding RMON events.

Procedure Steps

Step	Action
1	Enter Privileged Executive mode.
2	Enter the **show rmon event** command.

--End--

Viewing RMON history

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

Procedure Steps

Step	Action
1	Enter Privileged Executive mode.
2	Enter the **show rmon history [<port>]** command.

--End--

Variable Definitions

The following table describes the command variables.

Variable	Definition
<port>	The specified port number for which RMON history settings is displayed.

Viewing RMON statistics

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

Procedure Steps

Step	Action
1	Enter Privileged Executive mode.
2	Enter the **show rmon stats** command.

--End--

Setting RMON alarms

Use the following procedure to set

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.

--End--

Variable definitions

The following table describes the command variables.

Parameter	Description
<1-65535>	Unique index for the alarm entry.
<WORD>	The MIB object to be monitored. This object identifier can be 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 after the rising threshold is crossed. If omitted, or if an invalid event entry is referenced, no event is triggered.
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 after the falling threshold is crossed. If omitted, or if an invalid event entry is referenced, no event is triggered.
[owner <LINE>]	Specify an owner string to identify the alarm entry.

Deleting RMON alarm table entries

Use the following procedure to delete RMON alarm table entries.

Procedure Steps

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

--End--

Variable definitions

The following table describes the command parameters.

Variable	Definition
[<1-65535>]	The number assigned to the alarm. If no number is selected, all RMON alarm table entries are deleted.

Configuring RMON event log and traps

Use the following 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.

--End--

Variable definitions

The following table describes the command parameters.

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

Deleting RMON event table entries

Use the following procedure to clear entries in the table.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **no rmon event [<1-65535>]** command to delete the entries.

--End--

Variable definitions

The following table describes the command parameters.

Variable	Definition
[<1-65535>]	Unique identifier of the event. If not given, all table entries are deleted.

Configuring RMON history

Use the following 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 to configure the RMON history..

--End--

The **rmon history** command is executed in the Global Configuration command mode.

Variable definitions

The following table describes the command variables

Table 17
rmon history parameters

Parameter	Description
<1-65535>	Unique index for the history entry.
<LINE>	Specify 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>]	Specify an owner string to identify the history entry.

Deleting RMON history table entries.

Use this procedure to delete RMON history table entries.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.

2 Enter the **no rmon history [<1-65535>]** command to delete the entries.

--End--

Variable definitions

The following table describes the command parameters.

Variable	Definition
[<1-65535>]	Unique identifier of the event. If not given, all table entries are deleted.

Configuring RMON statistics

Use this procedure to configure RMON statistics settings.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the **rmon stats <1-65535> <LINE> [owner <LINE>]** command to configure RMON statistics.

--End--

Variable definitions

The following table describes the command variables.

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

Disabling RMON statistics

Use this procedure to disable RMON statistics. If the variable is omitted, 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 to disable RMON statistics.

--End--

Variable definitions

The following table describes the command parameters.

Variable	Definition
<1-65535>	Unique index for the statistics entry. If omitted, all statistics are disabled.

RMON configuration using Device Manager

Configuring RMON with the Device Manager

This section describes the configuration and management of RMON using Device Manager.

Working with RMON information

RMON information is viewed by looking at the graphing information associated with the port or chassis.

Viewing statistics

The DM gathers 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.

To view RMON ethernet statistics:

Procedure Steps

Step	Action
1	Select a port.
2	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.
3	The Graph Port window appears. Click the **RMON** tab.

--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 were directed to the broadcast address. This does not include multicast packets.
MulticastPkts	The total number of good packets received that were 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 were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
OversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
Fragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Normal behavior for etherStatsFragments is 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 were 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 a 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) that were transmitted and received on this port between 1 and 64 octets in length (excluding framing bits but including FCS octets).

Field	Descriptions
65..127	The total number of packets (including bad packets) that were 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) that were 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) that were 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) that were 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) that were 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: 10s
	Range: None, 2s, 5s, 10s, 30s, 1m, 5m, 30m 1h
Absolute	The total count since the last time counters were reset. A system reboot resets all counters.
Cumulative	The total count since the statistics tab was first opened. The elapsed time for the cumulative counter is shown at the bottom of the graph window.
Average/sec	The cumulative count divided by the cumulative elapsed time.
Min/sec	The minimum average for the counter for a polling interval over the cumulative elapsed time.
Max/sec	The maximum average for the counter for a polling interval over the cumulative elapsed time.
Last/sec	The average for the counter over the last polling interval.

Viewing 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:

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

Both the time interval and the number of buckets is configurable. After the last bucket is reached, bucket 1 is dumped and "recycled" to hold a new bucket of statistics. Then bucket 2 is dumped.

Use the following procedure to view RMON history.

Procedure Steps

Step	Action
1	Open the RmonControl window by selecting **Serviceability, RMON, Control** from the menu.
2	Select the **History** tab.

--End--

Job aid The following table describes the fields on the History tab.

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

Field	Description
	network, the etherHistoryOctets counter could overflow in about one hour at the Ethernet's maximum utilization.
Owner	The network management system that created this entry.

Creating a history

RMON can be used to collect statistics at intervals. For example, if switch performance is monitored over a weekend, enough buckets to cover two days must be set aside. To do this, set the history to gather one bucket each hour, thus covering a 48-hour period. After history characteristics are set, they cannot be modified; the history must be deleted and another created.

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

Procedure Steps

Step	Action
1	Open the RmonControl window by selecting **Serviceability, RMON, Control** from the menu.
2	Click **Insert**. The **Insert History** window appears.
3	In the fields provided, enter the information for the new RMON history.
4	Click **Insert**.

--End--

Job aid The following table describes the History tab of the RmonControl dialog box.

Field	Description
Index	A unique value assigned to each interface. An index identifies an entry in a table.
Port	Any Ethernet interface on the device.
BucketsRequested	The requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this entry.

Field	Description
BucketsGranted	The number of discrete sampling intervals over which data is saved in the part of the media-specific table associated with this entry. There are instances after the actual number of buckets associated with this entry is less than the value of this object. In this case, at the end of each sampling interval, a new bucket is added to the media-specific table.
Interval	The interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this entry. You can set this interval to a number of seconds between 1 and 3600 (1 hour). Because the counters in a bucket may overflow at their maximum value with no indication, note the possibility of overflow in the associated counters. Consider the minimum time in which a counter could overflow on a particular media type and set the historyControlInterval object to a value less than this interval. This interval is typically most important for the octets counter in a media-specific table. For example, on an Ethernet network, the etherHistoryOctets counter could overflow in about one hour at the Ethernet's maximum utilization.
Owner	The network management system that created this entry.

Disabling history

To disable RMON history on a port:

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

--End--

Viewing RMON history statistics

Use the following procedure to display Rmon History statistics.

Step	Action
1	Open the **RmonControl** window by selecting **Serviceability, 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 window fields.

Field	Description
SampleIndex	Indicates the sample number. As history samples are taken, they are assigned greater sample numbers.
Utilization	Estimates the percentage of a link's capacity that was 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 were destined for the broadcast 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 were dropped because of system resource constraints.
CRCAlignErrors	The number of packets received during a sampling interval that were between 64 and 1518 octets long. This length included 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 non-integral number of octets (Alignment Error).
UndersizePkts	The number of packets received during the sampling interval were less than 64 octets long (including FCS octets, but not framing bits.
OversizePkts	The number of packets received during the sampling interval were longer than 1518 octets (including FCS octets, but not framing bits, and were otherwise well formed.
Fragments	The number of packets received during the sampling interval were less than 64 octets long (including FCS octets, but not framing bits. The packets had a bad FCS with either an integral number of octects (FCS Error), or a non-integral 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

To gather ethernet statistics:

Procedure Steps

Step	Action
1	Open the **RmonControl** window by selecting **Serviceability, RMON, Control** from the menu.
2	Select the **Ether Stats** tab.
3	Select an **Index** and click **Insert**. The **Insert Ether Stats** window appears.
4	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.
5	Enter the owner of this RMON entry in the **Owner** field.
6	Click **Insert**.

--End--

Job aid The following table describes the **Ether Stats** tab fields.

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

Disabling Ethernet statistics gathering

Use this procedure to disable Ethernet statistics.

Step	Action
1	Open the **RmonControl** window by selecting **Serviceability, 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--

Alarm Manager

This section describes the use of Alarm Manager using DM.

Creating an Alarm

Use the following procedure to create an alarm to receive statistics and history using default values.

Step	Action
1	Selecting **Serviceability, RMON, Alarm Manager** from the menu.
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 three 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 (.). A card number, STG ID, IP address, or EtherStat information must be entered. • 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 18
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 the user must specify the index. This index 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 results in display of the port selection tool.

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

Deleting an alarm

Use the following procedure to delete an alarm.

Step	Action
1	Open the **Alarms** window by selecting **Serviceability, RMON, Alarms** from the menu.
2	Select the alarm to be deleted.
3	Click **Delete**.

--End--

Job aid The following table describes the fields on the **Alarms** tab.

Table 19
Alarms 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.

Field	Description
Interval	The interval in seconds over which data is sampled and compared with the rising and falling thresholds. After setting this variable, in the case of deltaValue sampling, you should set the interval short enough that the sampled variable is very 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) may be sampled.
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 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 value is compared with the rising and falling thresholds. The value during the current sampling period is not made available until the period is completed and remains available until the next period is completed.
StartupAlarm	The alarm that may be sent after this entry is first set to Valid. If the first sample after this entry becomes valid is greater than or equal to the risingThreshold and alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3), a single rising alarm is generated. If the first sample after this entry becomes valid is less than or equal to the fallingThreshold and alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3) a single falling alarm is generated.
RisingThreshold	A threshold for the sampled statistic. After the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, 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 after a rising threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry 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.

Field	Description
FallingThreshold	A threshold for the sampled statistic. After the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, 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.
FallingEventIndex	The index of the eventEntry that is used after a falling threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry 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.
Owner	The network management system that created this entry.
Status	The status of this alarm entry.

Events

This section describes how RMON events and alarms work together to provide notification after values in the network are outside of a specified range. After values pass the specified ranges, the alarm is triggered. The event specifies how the activity is recorded.

How events work

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

- RisingEvent
- FallingEvent

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

Viewing an event

Use the following procedure to view a table of events:

Procedure Steps

Step	Action
1	Select **Serviceability, RMON, Alarms** from the menu.

2 Select the **Events** tab.

--End--

Job aid The following table describes the **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 after the appropriate conditions occur.
Description	Specifies whether the event is a rising or falling event.
Type	The type of notification that the Device Manager provides about this event. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations. Possible notifications 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 generated events, this value is zero.
Owner	If traps are specified to be sent to the owner, this is the name of the machine which receives traps.

Creating an event

Use the following procedure to create an event.

Procedure Steps

Step	Action
1	Select **Serviceability, RMON, Alarms** from the menu.
2	Select the **Events** tab.
3	Click **Insert**. The **Insert Events** window appears.
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--

Job aid The following table describes the **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 after the appropriate conditions occur.
Description	Specifies whether the event is a rising or falling event.
Type	The type of notification that the Device Manager provides about this event. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations. Possible notifications 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 generated events, this value is zero.
Owner	If traps are specified to be sent to the owner the name of the machine receives alarm traps.
Status	Normally valid. A not-valid field indicates that an SNMP agent other than the Device Manager has tried to modify an RMON parameter or that network conditions have corrupted an SNMP packet sent by the Device Manager. The status temporarily appears as "under creation" and then the status becomes either "valid" or the field is deleted.

Deleting an event

Use the following procedure to delete an event.

Step	Action
1	Select **Serviceability, RMON, Alarms** from the menu.
2	Select the **Events** tab.
3	Select an event from the list.

4 Click **Delete**.

--End--

Job aid The following table describes the **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 after the appropriate conditions occur.
Description	Specifies whether the event is a rising or falling event.
Type	The type of notification that the Device Manager provides about this event. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations. Possible notifications 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 generated events, this value is zero.
Owner	If traps are specified to be sent to the owner the name of the machine receives alarm traps.
Status	Normally valid. A not-valid field indicates that an SNMP agent other than the Device Manager has tried to modify an RMON parameter or that network conditions have corrupted an SNMP packet sent by the Device Manager. The status temporarily appears as "under creation" and then the status becomes either "valid" or the field is deleted.

Viewing log information

Use the following procedure to view the alarm activity.

Procedure Steps

Step	Action
1	Select **Serviceability, RMON, Alarms** from the menu.
2	Select the **Log** tab.

--End--

Job aid

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

Item	Description
Time	Specifies the time an event occurred that activated the log entry.
Description	Specifies whether the event is a rising or falling event.

RMON configuration using Web-based management

Configuring RMON with the Web-based management

This section discusses the configuration and management of RMON using the Web-based management.

Configuring RMON alarm parameters

Alarms are used to alert you after the value of a variable goes out of range. RMON alarms can be defined on a MIB variable that resolves to an integer value. String variables (such as system description) cannot be used as alarm variables.

Creating an RMON alarm

Use the following procedure to configure an RMON fault threshold.

Step	Action
1	Select **Fault, RMON Alarm** from the menu.
2	In the fields provided in the **RMON Alarm Creation** section, enter the information for the new threshold.
3	Click **Submit**.

--End--

The new RMON alarm is displayed in the **RMON Alarm Table** section.

Job aid The following tables outlines the fields in this section.

Field	Description
Alarm Index	Type the unique number to identify the alarm entry.
Interval	Type the time period (in seconds) to sample data and compare the data to the rising and falling thresholds.
Unit	Choose the unit on which to set the alarm

Field	Description
Port	Choose the port on which to set an alarm.
Parameter	Choose from the sampled statistics supported in web.
Alarm Sample	Choose 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. You can create 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 delta-valued alarm and add them together, the result is twice the actual value. (This result is not an error in the software.)
Rising Level	The value of the rising threshold.
Rising Event Index	The event entry to be used after the rising level is crossed.
Falling Level	The value of the falling threshold
Falling Event Index	The event entry to be used after the falling level is crossed.
Owner	Owner information.

Deleting an RMON alarm configuration

Use the following procedure to delete an existing RMON alarm configuration.

Step	Action
1	Select **Fault, RMON Alarm** from the menu.
2	In the **RMON Alarm Table**, click the **Delete** icon in the row of the entry to be deleted.
3	A message prompts for confirmation of the request. Click **Yes**.

--End--

Job aid

The following tables outlines the fields in this section.

Field	Description
Alarm Index	Type the unique number to identify the alarm entry.
Port	Choose the port on which to set an alarm.
Parameter	Choose the sampled statistic.
Rising Level	Type the event entry to be used after a rising threshold is crossed.
Falling Level	Type the event entry to be used after a falling threshold is crossed.
Rising Action	Choose 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	Type the time period (in seconds) to sample data and compare the data to the rising and falling thresholds.
Alarm Sample	Choose 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. You can create 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 delta-valued alarm and add them together, the result is twice the actual value. (This result is not an error in the software.)

Creating events

Use this procedure to create an RMON event to use with alarms

Procedure Steps

Step	Action
1	Open the RMON Event window by selecting **Fault, RMON Event**.

2 In the RMON Event Creation section, enter the required information and select an action to be performed by the event, either generate a log entry, send a snmp trap, or both.

3 Click **Submit** to save the setting.

--End--

Viewing the RMON fault event log

RMON events and alarms work together to produce notification after values in the network go out of a specified range. After 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. After RMON is globally enabled, two default events are generated:

- Rising Event
- Falling Event

Default events specify that after an alarm goes out of range, the firing of the alarm is tracked in both a trap and a log. For example, after an alarm fires at the rising threshold, the rising event specifies that this information be sent to both a trap and a log. The **RMON Event Log** window works in conjunction with the **RMON Alarm** window to enable viewing the history of RMON fault events.

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

Procedure Steps

Step	Action
1	Select **Fault, RMON Event Log** from the menu.
2	Observe the RMON Event Log information.

--End--

IPFIX Configuration using NNCLI

This section describes the commands used in the configuration and management of IP Flow Information Export (IPFIX) using the NNCLI.

Configuring IPFIX collectors

The **ip ipfix collector** command is used to configure IPFIX collectors. IPFIX collectors are used to collect and analyze data exported from an IPFIX compliant switch. In Software Release 5.0, the only external collector supported is **NetQOS**. At this time, up to two collectors can be supported.

IPFIX data is exported from the switch in *Netflow version 9* format. Data is exported using UDP port 9995.

IPFIX data is not load balanced when two collectors are in use. Identical information is sent to both collectors.

Use the following procedure to configure the IPFIX collectors.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Use the **ip ipfix collector <unit_number> <collector_ip_address>** command to configure the IPFIX collector.

--End--

The **ip ipfix collector** command is executed in the Global Configuration mode.

Variable definitions

The following table describes the parameters for this command.

Parameter	Description
<unit_number>	The unit number of the collector. Currently up to two collectors are supported so the values 1 or 2 are valid.
<collector_ip_address>	The IP address of the collector.

Enabling IPFIX globally

Use the following procedure to globally enable IPFIX on the switch.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Use the **ip ipfix enable** command to enable IPFIX on the switch.

--End--

Configuring unit specific IPFIX

Use the following command to configure unit specific IPFIX parameters.

Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Use the **ip ipfix slot <unit_number> [aging-interval <aging_interval>] [export-interval <export_interval>] [exporter-enable] [template-refresh-interval <template_refresh_interval>] [template-refresh-packets <template_refresh_packets>]** command to enable IPFIX on the switch.

--End--

Variable definitions

The parameters of this command are described in the following table.

Parameter	Description
<unit_number>	The unit number of the collector. Currently up to two collectors are supported so the values 1 or 2 are valid.

Parameter	Description
<aging_interval>	The IPFIX aging interval. This value is in seconds from 0 to 2147400.
<export_interval>	The IPFIX export interval. This interval is the value at which IPFIX data is exported in seconds from 10 to 3600.
<template_refresh_interval>	The IPFIX template refresh interval. This value is in seconds from 300 to 3600.
<template_refresh_packets>	The IPFIX template refresh packet setting. This value is the number of packets from 10000 - 100000.

Enabling IPFIX on the interface

Use the following procedure to enable IPFIX on the interface.

Procedure Steps

Step	Action
1	Enter Interface Configuration mode.
2	Use the **ip ipfix enable** command to enable IPFIX on the interface.

--End--

Enabling IPFIX export through ports

Use the following procedure to enable the ports exporting data through IPFIX.

Procedure Steps

Step	Action
1	Enter Interface Configuration mode.
2	Use the **ip ipfix port <port_list>** command to enable IPFIX on the interface.

--End--

Variable definitions

The following table describes the command parameters

Variable	Definition
port-list	Single or comma-separated list of ports.

Deleting the IPFIX information for a port

Use the following procedure to delete the collected IPFIX information for a port.

Procedure Steps

Step	Action
1	Enter Privileged Executive mode.
2	Use the **ip ipfix flush port <port_list> [export-and-flush]** command to delete the collected IPFIX information for the port or ports.

--End--

Variable definitions

The following table describes the command parameters.

Variable	Definition
port-list	Single or comma-separated list of ports.
export-and-flush	Export data to a collector before it is deleted.

Viewing the IPFIX table

Use the following procedure to display IPFIX data collected from the switch.

Procedure Steps

Step	Action
1	Enter Privileged Executive mode.
2	Use the **show ip ipfix table <unit_number> sort-by <sort_by> sort-order <sort_order> display <num_entries>** command view the IPFIX data.

--End--

Variable definitions

The following table describes the command parameters.

Variable	Definition
<unit_number>	The unit number of the collector. Currently up to two collectors are supported so the values 1 or 2 are valid.
<sort_by>	The value on which the data is sorted. Valid options are: • byte-count • dest-addr • first-pkt-time • last-pkt-time • pkt-count • port • protocol • source-addr • TCP-UDP-dest-port • TCP-UDP-src-port • TOS
<sort_order>	The order in which the data is sorted. Valid options are ascending and descending.
<num_entries>	The number of data rows to display. Valid options are: • all • top-10 • top-25 • top-50 • top-100 • top-200

IPFIX configuration using Device Manager

This section describes the configuration and management of IPFIX functionality using the Device Manager.

Global IPFIX configuration

IPFIX functionality can be globally enabled or disabled from the Device Manager. By default, IPFIX is disabled and must be enabled before it starts to collect flow information. This section contains the procedures for enabling and disabling IPFIX on a switch.

Global configuration using the DM

Use the following command to enable or disable IPFIX using the DM

Procedure Steps

Step	Action
1	Select **Serviceability, IPFIX** from the Device Manager menu. The **IPFIX** dialog opens with the **Global** tab selected..
2	On the **Global** tab, select the operational state of IPFIX functionality from the **State** area.
3	Click **Apply**.

--End--

Configuring IPFIX flows

After IPFIX has been enabled on a switch, the ports IPFIX monitors must be configured. Configuration of flow information sources is performed in the Device Manager.

Configuring flows using DM

To configure IPFIX flows in the DM, perform the following procedure:

Step	Action
1	Select **Serviceability, IPFIX** from the Device Manager menu. The IPFIX dialog opens with the Global tab selected.
2	Select the **Exporters** tab.
3	The **Exporters** tab lists the IPFIX exporters that are currently available. If connected to a stand-alone unit, the export properties of that unit are listed. If connected to a stack, the export properties of all units in the stack are listed.
4	Configure the IPFIX export properties.
5	Click **Apply**.
6	Continue with the export configuration process.

--End--

Job aid

The following table describes the fields in the tab.

Field	Description
Slot(Unit)	The switch that is exporting IPFIX flows. This number corresponds to the unit number in a stack or is 1 for a stand-alone unit.
AgingIntv	The aging interval of the flow record in seconds. This value is an integer between 0 and 2147400.
ExportIntv	The frequency of data exports to the collector in seconds. This value is an integer between 10 and 3600.
ExportState	The current state of the exporter.
TempRefIntvSec	The template refresh time out in seconds. The template is sent out to the collector either at the interval specified in this value or after the number of packets specified in the **TempRefIntvPkts** value, whichever occurs first. This value is an integer between 300 and 3600.
TempRefIntvPkts	The template refresh time out in numbers of packets. The template is sent out to the collector either at the interval specified in this value or after the number of seconds specified in the **TempRefIntvSec** value, whichever occurs first. This value is an integer between 10000 and 100000.
ActiveTimeout	Flow record active timeout value in minutes.

Configuring IPFIX collectors

IPFIX collectors are used to collect and analyze data exported from an IPFIX-compliant switch. In Software Release 5.0, the only external collector supported is **NetQOS**. At this time, up to two collectors can be supported.

IPFIX data is exported from the switch in *Netflow version 9* format. Data is exported using UDP port 9995.

IPFIX data is not load balanced when two collectors are in use. Identical information is sent to both collectors.

Use the following procedure to configure an IPFIX collector.

Procedure Steps

Step	Action
1	Select **Serviceability, IPFIX** from the Device Manager menu. The **IPFIX** dialog opens with the **Global** tab selected.
2	Select the **Collectors** tab.
3	To modify the configuration of a collector, use the fields provided on the tab.
4	To create a new collector, click **Insert**.
5	The **Insert Collectors** dialog appears.
6	Using the fields provided on the **Insert Collectors** dialog, configure the new collector.

--End--

Job aid

The following table describes the fields on the collectors tab.

Field	Description
Slot(Unit)	The unit number of the collector. Currently up to two collectors are supported.
AddressType	The address type of the IP address of the collector. Currently only IPv4 addresses are supported.
Address	The IP address of the collector.
Protocol	The protocol used to transport the IPFIX data to the collector. Currently only the UDP protocol is supported for this task.

Field	Description
DestPort	The port on which the collector is listening for IPFIX data. Currently only port 9995 is supported for this task.
ExporterIpType	The address type of the IP address of the IPFIX exporter. Currently only IPv4 addresses are supported.
ExporterIp	The IP address of the IPFIX exporter.
ProtoVer	The format in which IPFIX data is provided to the collector. Currently only Netflow version 9 formatting is supported for this task.
Enable	The operational state of this collector.

The following table describes the fields in the Insert Collectors dialogue.

Field	Description
Slot(Unit)	The unit number of the collector. Currently up to two collectors are supported so the values 1 or 2 are valid.
AddressType	The address type of the IP address of the collector. Currently only IPv4 addresses are supported.
Address	The IP address of the collector.
Protocol	The protocol used to transport the IPFIX data to the collector. Currently only the UDP protocol is supported for this task.
DestPort	The port on which the collector is listening for IPFIX data. Currently only port 9995 is supported for this task.
ProtoVer	The format in which IPFIX data is provided to the collector. Currently only Netflow version 9 formatting is supported for this task.
Enable	The operational state of this collector.

Configuring IPFIX ports

Use the **Ports** tab to configure port settings for IPFIX data export. To configure IPFIX ports, use the following procedure:

Step	Action
1	Select **Serviceability, IPFIX** from the Device Manager menu. The **IPFIX** dialog opens with the **Global** tab selected.
2	Select the **Ports** tab. This tab is used to configure the individual ports on the exporting units.
3	Using the fields provided, configure the IPFIX parameters for the individual ports.

If a single port is selected, packets are sampled every second. If multiple ports are selected, sampling is performed on every port that has a link in succession. Sampling rotates between the selected ports with each port having a sampling time of 1 second. For example, if 10 ports were selected on a switch, each port is sampled every 10 seconds.

4 Click **Apply**.

--End--

Job aid

The following table describes the fields on the Ports tab.

Field	Description
Id	The individual port on which the IPFIX parameters are being configured. Ports are itemized in the format *Unit* / *Port*.
Flush	Determines the flushing action to take on the port. Flushing the port of data involves deleting all previously gathered infotmation about that port. This field provides three options: • none - The port data is not flushed. • flush - The port data is flushed; deleting it from switch memory. • exportAndFlush - The port data is exported to a configured collector and the data is then flushed. Although this field is displayed on a per port basis, flushing is only supported on a per unit basis in Software Release 5.0.
AllTraffic	Determines whether IPFIX data is collected on this port. This field provides two options: • enable - IPFIX data is collected. • disable - IPFIX data is not collected.

Graphing Exporter Statistics

Use the following procedure to view IPFIX exporter statistics.

Procedure Steps

Step	Action
1	Select **Serviceability, IPFIX** from the Device Manager menu. The IPFIX dialog opens with the Global tab selected.
2	Select the **Collectors** tab.

3 On the Collectors tab, select an entry and click **Graph**. The IPFIX Exporter Stats window opens with the Exporter tab selected.

--End--

Job aid

The following table outlines the fields on this tab.

Field	Description
OutPkts	Indicates the total number of packets sent.
OutOctets	Indicates the total number of bytes sent.
PktsLoss	Indicates the total number of records lost.

Exporter Stats Clear Time

In conjunction with the Exporters tab, the Clear Time tab indicates the system time after exporter statistics were last cleared (none if this has never occurred).

IPFIX configuration using the Web-based management

This section outlines the configuration of IPFIX using Web-based management.

Global configuration using the Web-based management

IPFIX functionality can be globally enabled or disabled from the Web-based management. By default, IPFIX is disabled and must be enabled before it will start to collect flow information. This section contains the procedures for enabling and disabling IPFIX on a switch.

Use this procedure to enable or disable IPFIX using the Web-based management.

Procedure

Step	Action
1	Select **Applications, IP Fix, IP Fix Configuration** from the Web-based management navigation pane. The IP Fix Configuration page appears.
2	Select the operational state of the IPFIX functionality from the IP Fix drop down list in the IP Fix Global Setting area.
3	Click **Submit**.

--End--

Configuring flows using the Web-based management

After IPFIX has been enabled on a switch, the ports IPFIX will monitor must be configured. Configuration of flow information sources can be performed in the Web-based management.

Flow configuration in the Web-based management is performed on the **IP Fix Configuration** page.

Use the following procedure to configure IPFIX flows using the Web-based management.

Procedure Steps

Step	Action
1	Select **Applications, IP Fix Configuration** from the Web-based management navigation pane. The IP Fix Configuration page appears.
2	Using the fields provided in the IP Fix Port Setting area, configure the IPFIX flow for individual ports.
3	Click **Submit**.

--End--

Job aid

The following table describes the fields on this page.

Field	Description
Aging Time	The aging interval of the flow record in seconds.
Observation Ports	Each port is represented by a check box. Select or de-select the appropriate check boxes to enable or disable IPFIX data collection on that port. Select or de-select all ports using the **All** check box.

Viewing IPFIX data

IPFIX data can be viewed using the Web-based management. This viewing mechanism is provided for you to or not have IPFIX collectors configured on the network. Using this interface, data can be sorted, filtered, and cleared entirely.

Use the following procedure to view IPFIX data.

Procedure Steps

Step	Action
1	Choose **Applications, IP Fix, IP Fix Information** from the Web-based management navigation pane. The **IP Fix Information** page appears.
2	Using the fields provided in the **IP Fix Information (View By)** area, configure the viewing or clearing of the IPFIX data.
3	Click **Submit**.

4 The IPFIX data with be filtered and sorted based on the selections.

--End--

Job aid

The following table describes the fields on the IPFIX Information page.

Field	Description
Sort On	The item of data to sort the IPFIX data on. IPFIX data can be sorted on any item that is gathered.
Sort Order	The order to apply to the sorted data.
Entries To Display	The number of entries to display.
Clear Statistics	Whether or not to clear the current statistics from memory.

Nortel Ethernet Routing Switch 5000 Series

Configuration — System Monitoring

Release: 6.1
Publication: NN47200-505
Document revision: 05.01
Document release date: 25 May 2009

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

www.nortel.com

NORTEL