



Nortel Ethernet Routing Switch 2500 Series

# Configuration — System Monitoring

Document status: Standard  
Document version: 03.01  
Document date: 27 October 2008

Copyright © 2007-2008, Nortel Networks  
All Rights Reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

## **Trademarks**

\*Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

Adobe and Adobe Reader are trademarks of Adobe Systems Incorporated.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

Trademarks are acknowledged with an asterisk (\*) at their first appearance in the document.

All other trademarks are the property of their respective owners.

## **Restricted rights legend**

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

---

# Contents

---

<b>New in this release</b>	<b>7</b>
Features	7
<b>Introduction</b>	<b>9</b>
NNCLI command modes	9
<b>System Monitoring Fundamentals</b>	<b>11</b>
CPU and memory utilization	11
Trap Web page	12
Light Emitting Diode display	12
System Log	12
Port mirroring	12
Port mirroring configuration rules	13
Stack monitor	14
Chassis and port statistics	14
Remote Monitoring	15
RMON alarms	15
<b>Network monitoring configuration using NNCLI</b>	<b>19</b>
CPU utilization	19
Memory utilization	19
System log	20
Viewing the system event log	20
Configuring system logging	21
Disabling logging	22
Setting default logging	22
Clearing log messages	22
Port mirroring	23
Displaying the port-mirroring configuration	23
Configuring port-mirroring	24
Disabling port-mirroring	24
Port statistics	24
Displaying port-statistics	25
Clearing statistical information	26
Stack health	27
Viewing stack health	27

---

Viewing stack monitor information	27
Configuring the stack monitor	28
Disabling the stack monitor	28
<b>Network monitoring configuration using Device Manager</b>	<b>29</b>
CPU and memory utilization	29
Viewing the system log settings	30
Viewing the Remote System Log tab	32
Graphing chassis statistics	33
Viewing IP statistics	34
Viewing ICMP In statistics	36
Viewing ICMP Out statistics	37
Viewing TCP statistics	38
Viewing UDP statistics	40
Graphing port statistics	41
Graphing the Interface tab	41
Graphing the Ethernet Errors tab	43
Misc. Stats tab	46
Configuring the stack monitor	47
<b>Network monitoring configuration using Web-based management</b>	<b>49</b>
CPU and memory utilization	49
Using the trap Web page to identify trap receivers	49
Stack Health	50
Viewing the system log	51
Configuring port mirroring	52
Viewing statistics	53
Viewing port statistics	53
Zeroing ports	56
Zeroing all ports	56
Viewing interface statistics	57
Viewing Ethernet error statistics	58
Viewing transparent bridging statistics	59
Monitoring MLT traffic	60
<b>RMON using the NNCLI</b>	<b>63</b>
Viewing the RMON alarms	63
Viewing the RMON events	64
Viewing the RMON history	64
Viewing the RMON statistics	64
Configuring RMON alarms	65
Deleting RMON alarms	66
Configuring RMON events settings	66
Deleting RMON events settings	67
Configuring RMON history settings	67

---

---

Deleting RMON history settings	68
Configuring RMON statistics settings	69
Deleting RMON statistics	69

---

## **RMON using Device Manager** **71**

Working with RMON information	71
Viewing statistics	71
Viewing history	74
Creating history items	74
Disabling history	76
Viewing RMON history statistics	77
Enabling Ethernet statistics gathering	78
Disabling Ethernet statistics gathering	79
Creating an alarm	79
Deleting an alarm	81
Viewing RMON statistics and history	82
Using RMON events	84
Viewing an event	84
Deleting an event	86
Viewing RMON log information	86

---

## **RMON using Web-based management** **89**

Configuring RMON fault threshold parameters	89
Creating an RMON fault threshold	89
Deleting an RMON threshold configuration	92
Viewing the RMON fault event log	93
Viewing RMON Ethernet statistics	94
Viewing RMON history	95



---

## New in this release

---

The following sections detail what's new in *Configuration — System Monitoring* (NN47215-502) for Release 4.2:

### Features

For information about changes that are feature related, see the section:

- ["Stack monitor" \(page 14\)](#)
- ["Stack health" \(page 27\)](#)
- ["CPU and memory utilization" \(page 11\)](#)
- ["Trap Web page " \(page 12\)](#)
- ["System Log" \(page 12\)](#)





---

# Introduction

---

This guide provides information about system logging, displaying system statistics, and configuring network monitoring on the Nortel Ethernet Routing Switch 2500 Series. This guide describes the features of the following Nortel switches.

- Nortel Ethernet Routing Switch 2526T
- Nortel Ethernet Routing Switch 2526T-PWR
- Nortel Ethernet Routing Switch 2550T
- Nortel Ethernet Routing Switch 2550T-PWR

The term "Ethernet Routing Switch 2500 Series" is used in this document to describe the features common to the switches mentioned above.

A switch is referred to by its specific name while describing a feature exclusive to the switch.

## NNCLI command modes

NNCLI provides the following command modes:

- User EXEC
- Privileged EXEC
- Global Configuration
- Interface Configuration

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

If no password is set, you can enter NNCLI in User EXEC mode and use the **enable** command to move to the next level (Privileged EXEC mode). However, if you have read-only access, you cannot progress beyond User EXEC 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 EXEC 2526T>	No entrance command, default mode	<b>exit</b> or <b>logout</b>
Privileged EXEC 2526T#	<b>enable</b>	<b>exit</b> or <b>logout</b>
Global Configuration 2526T(config)#	From Privileged EXEC mode, enter: <b>configure</b>	To return to Privileged EXEC mode, enter: <b>end</b> or <b>exit</b>  To exit NNCLI completely, enter: <b>logout</b>
Interface Configuration 2526T(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: <b>exit</b>  To return to Privileged EXEC mode, enter: <b>end</b>  To exit NNCLI completely, enter: <b>logout</b>

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

---

# System Monitoring Fundamentals

---

The Ethernet Routing Switch 2500 Series provide features that allow you to monitor your network, display switch statistics, log system events, and provide Remote Network Monitoring (RMON). This chapter contains information about the following topics:

## Navigation

- ["CPU and memory utilization" \(page 11\)](#)
- ["Trap Web page " \(page 12\)](#)
- ["Light Emitting Diode display" \(page 12\)](#)
- ["System Log" \(page 12\)](#)
- ["Port mirroring" \(page 12\)](#)
- ["Stack monitor" \(page 14\)](#)
- ["Chassis and port statistics" \(page 14\)](#)
- ["Remote Monitoring" \(page 15\)](#)

## 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), 1minute (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.

### Trap Web page

Trap Web page in Web-based management provides a graphical method to enable or disable traps you want to send. In the case multiple trap receivers are selected you can map which traps are sent to which receiver. You can group traps by event type to send to persons who have roles such as security or network connectivity.

You can access a Web page, for every host, from which you can enable or disable every trap for a specific host. The access to those pages is through the SNMP Trap Web page, which page 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.

### Light Emitting Diode display

The ERS 2500 Series displays diagnostic and operation information through the LEDs on the unit. Familiarize yourself with the interpretation of the LEDs on the 2500 series device. See *Nortel Ethernet Routing Switch 2500 Series — Installation* (NN47205-300) for detailed information regarding the interpretation of the LEDs.

### System Log

The System Log displays messages obtained from system Non Volatile Random Access Memory (NVRAM) or Dynamic Random Access Memory (DRAM). The System Log displays only the data for the Ethernet Routing Switch 2500 Series through the Console or Comm port, WEB, or Telnet.

System Log messages operate as follows:

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

### Port mirroring

The Port mirroring feature, also referred to as conversation steering, lets you allocate a single switch port (monitor port) as a traffic monitor for another switch port (mirror port). All incoming traffic on the mirrored port is copied to the monitor port. This operation excludes traffic forwarded by the switch. This feature is helpful in network troubleshooting.

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

Ethernet Routing Switch 2500 Series supports ingress, egress, and ingress/egress port-based mirroring.

### **Port mirroring configuration rules**

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

#### **Port mirroring ingress mode (XRX or ->Port X)**

In the Port mirroring ingress mode, packets received on mirror port X are copied to the monitor port.

##### ***Standalone***

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

##### ***Stack***

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

##### ***Duplex Stack***

Ingress port mirroring is not supported in duplex stacking.

#### **Port mirroring egress mode (XTX or Port X ->)**

In the Port mirroring egress mode, packets transmitted on mirror port X are copied to the monitor port.

##### ***Standalone***

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

##### ***Stack***

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

#### **Port mirroring ingress and egress mode (XRX or XTX or <->Port X)**

In the Port Mirroring ingress and egress mode, packets that are either transmitted or received on mirror port X are copied to the monitor port.

### ***Standalone***

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

### ***Stack***

Ingress and egress port mirroring is not supported in stack configurations.

## **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.

## **Chassis and port statistics**

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

## Remote Monitoring

RMON MIB is an interface between the RMON agent on an Ethernet Routing Switch 2500 Series and an RMON management application, such as the Device Manager.

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

The RMON agent continuously collects statistics and proactively monitors switch performance. You can view this data through the CLI, web-based management, and Device Manager.

RMON has three major functions:

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

### RMON alarms

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

All alarms share the following characteristics:

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

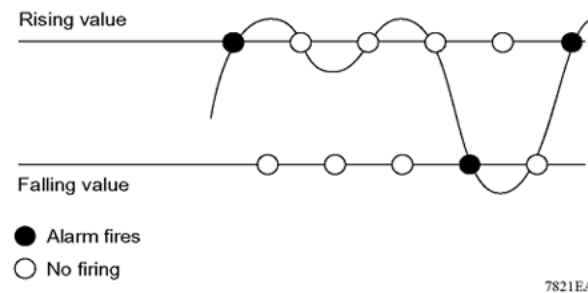
When alarms are activated, you can view the activity in a log or a trap log, or you can create a script to notify you by sending an audible sound to a console, sending e-mail, or calling a pager.

### How RMON alarms work

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

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

The following figure describes how alarms are triggered.



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.

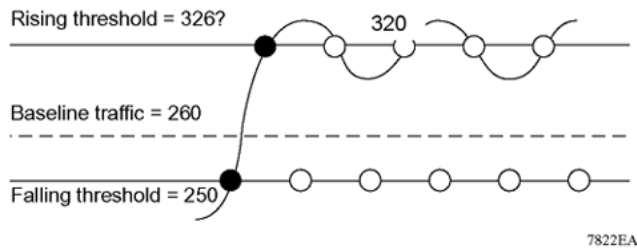
A general guideline is to define one of the threshold values to an expected baseline value, and then define the opposite threshold as the out-of-bounds limit. Because of sample averaging, the value may be equal to  $\pm 1$  of the baseline units. For example, assume an alarm is defined on octets going 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.)

## How events work

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

- RisingEvent
- FallingEvent

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

---

# Network monitoring configuration using NNCLI

---

This chapter describes how to configure network monitoring using NNCLI.

## Navigation

- ["CPU utilization" \(page 19\)](#)
- ["Memory utilization" \(page 19\)](#)
- ["System log" \(page 20\)](#)
- ["Port mirroring" \(page 23\)](#)
- ["Port statistics" \(page 24\)](#)
- ["Stack health" \(page 27\)](#)

## CPU utilization

Use this procedure to view CPU utilization.

### Procedure Steps

Step	Action
1	Enter Privileged exec mode.
2	Enter the <code>show cpu-utilization</code> command.
3	Observe the displayed information.
—End—	

## Memory utilization

Use this procedure to view memory utilization.

### Procedure Steps

Step	Action
1	Enter Privileged exec mode.
2	Enter the <code>show memory-utilization</code> command.
3	Observe the displayed information.
—End—	

## System log

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

### Navigation

- ["Viewing the system event log" \(page 20\)](#)
- ["Configuring system logging " \(page 21\)](#)
- ["Disabling logging" \(page 22\)](#)
- ["Disabling logging" \(page 22\)](#)
- ["Setting default logging " \(page 22\)](#)
- ["Clearing log messages" \(page 22\)](#)

### Viewing the system event log

The `show logging` command displays the configuration and the current contents of the system event log.

### Procedure Steps

Step	Action
1	Enter Privileged EXEC mode.
2	Enter the <code>show logging</code> command.
3	Observe the displayed information.
—End—	

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

## Variable definitions

The following table describes the command parameters

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

## Configuring system logging

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

### Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the <code>logging [enable   disable] [level critical   serious   informational   none] [nv-level critical   serious   none] remote [address   enable   level] volatile [latch   overwrite]</code> command.

—End—

## Variable definitions

The following table describes the command parameters.

Variable	Definition
enable   disable	Enables or disables the event log (enabled is the default setting).
level critical   serious   informational   none	Specify the level of logging stored in DRAM.
nv-level critical   serious   none	Specify the level of logging stored in NVRAM.

Variable	Definition
remote	Configure remote logging parameters. Address: configure remote syslog address. Enable: enable remote logging. Level: configure remote logging level.
volatile	Configure options for logging to DRAM. Latch: latch DRAM log when it is full. Overwrite: overwrite DRAM log when it is full.

### Disabling logging

Use this procedure to disable the system event log.

#### Procedure Steps

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | Enter Global Configuration mode.           |
| 2 | Enter the <code>no logging</code> command. |

—End—

### Setting default logging

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

#### Procedure Steps

Step	Action
------	--------

- |   |   |
|---|---|
| 1 | Enter Global Configuration mode.                |
| 2 | Enter the <code>default logging</code> command. |

—End—

### Clearing log messages

Use this procedure to clear all log messages in DRAM.

#### Procedure Steps

Step	Action
------	--------

- |   |                             |
|---|-----------------------------|
| 1 | Enter Privileged EXEC mode. |
|---|-----------------------------|

- 2 Enter the `clear logging [non-volatile] [nv] [volatile]` command.

---

—End—

---

### Variable Definitions

The following table describes the command parameters.

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

## Port mirroring

This section describes how to configure and display port mirroring

- ["Displaying the port-mirroring configuration" \(page 23\)](#)
- ["Configuring port-mirroring " \(page 24\)](#)
- ["Disabling port-mirroring" \(page 24\)](#)

### Displaying the port-mirroring configuration

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

#### Procedure Steps

Step	Action
------	--------

- |   |   |
|---|---|
| 1 | Enter Privileged exec mode.                         |
| 2 | Enter the <code>show port-mirroring</code> command. |
| 3 | Observe the displayed information.                  |

---

—End—

---

### Job aid

The following figure shows the command output.

```
2550T-PWR# show port-mirroring
Monitoring Mode: Disabled
2550T-PWR#
```

## Configuring port-mirroring

Use this procedure to configure port mirroring.

### Procedure Steps

Step	Action
1	Enter Privileged exec mode.
2	Enter the <code>port-mirroring</code> mode <code>{disable   Xrx Xtx Xrx-OrXtx}</code> <code>monitor-port &lt;portlist&gt; mirror-port-X &lt;portlist&gt;</code> command.
3	Observe the displayed information.

—End—

### Variable definitions

The following table describes the command variables.

Variable	Definition
disable	Disables port-mirroring.
Xrx	Mirror packets received on port X.
Xtx	Mirror packets transmitted on port X.
XrxOrXtx	Mirror packets received or transmitted on port X.

## Disabling port-mirroring

Use this procedure to disable port mirroring.

### Procedure Steps

Step	Action
1	Enter Privileged exec mode.
2	Enter the <code>no port-mirroring</code> command.

—End—

## Port statistics

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



## Navigation

- "Displaying port-statistics " (page 25)
- "Clearing statistical information" (page 26)

## Displaying port-statistics

Use this procedure to display port statistics.

### Procedure Steps

Step	Action
1	Enter Interface configuration mode.
2	Enter the <code>show port-statistics [port &lt;portlist&gt;]</code> command.
—End—	

## Variable definitions

The following table describes the command variables.

Variable	Definition
port <portlist>	<p>Specifies the port numbers to display statistics about.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="text-align: center;"><b>ATTENTION</b></p> <p>If you omit this parameter, the system uses the port number you specified when selecting the interface.</p> </div>

## Job aid

The following image is an example of the command output.

```

2550T-PWR#show port-statistics port 1/1
Received
Packets: 0
Multicasts: 0
Broadcasts: 0
Total Octets: 0
FCS Errors: 0
Undersized Packets: 0
Oversized Packets: 0
Filtered Packets: 0
Frame Errors: 0
Pause Frames: 0
Transmitted
Packets: 0
Multicasts: 0
Broadcasts: 0
Total Octets: 0
Collisions: 0
Single Collisions: 0
Multiple Collisions: 0
Excessive Collisions: 0
Deferred Packets: 0
Late Collisions: 0
Pause Frames: 0
Packets 64 bytes: 0
        65-127 bytes: 0
        128-255 bytes: 0
        256-511 bytes: 0
        512-1023 bytes: 0
        1024-1518 bytes: 0
        Jumbo: 0
Dropped On No Resources: 0

```

### Clearing statistical information

Use this command to clear all statistical information for the specified port and set all counters to zero (0).

### Procedure Steps

Step	Action
1	Enter Interface configuration mode.
2	Enter the <code>clear-stats [port &lt;portlist&gt;]</code> command.

—End—

### Variable definitions

The following table describes the command variables.

Variable	Definition
port <portlist>	<p>Specifies the port numbers to display statistics about.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="text-align: center;"><b>ATTENTION</b></p> <p>If you omit this parameter, the system uses the port number you specified when selecting the interface.</p> </div>

## Stack health

This section describes how you can view and configure stack health parameters.

### Navigation

- ["Viewing stack health" \(page 27\)](#)
- ["Viewing stack monitor information" \(page 27\)](#)
- ["Configuring the stack monitor" \(page 28\)](#)

### Viewing stack health

Use this procedure to display the stack health information.

#### Procedure Steps

Step	Action
------	--------

- |   |   |
|---|---|
| 1 | Enter the <code>show stack health</code> command. |
| 2 | Observe the NNCLI output.                         |

—End—

### Viewing stack monitor information

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

#### Procedure Steps

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | Enter the <code>show stack-monitor</code> command. |
| 2 | Observe the NNCLI output.                          |

---

—End—

---

### Configuring the stack monitor

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

#### Procedure Steps

Step	Action
1	Enter the <code>config stack-monitor {enable [stack-size &lt;2-8&gt;] [trap-interval &lt;30-300&gt;]}</code> command.
2	Observe the NNCLI output.

---

—End—

---

#### Variable definitions

The following table describes the command parameters.

Variable	Definition
enable	Enable stack monitoring.
stack-size <2-8>	Set stack size to be monitored in the range of 2 to 8.
trap-interval <30-300>	Set interval between traps in the range of 30 to 300 seconds.

### Disabling the stack monitor

Use this procedure to disable the stack monitor.

#### Procedure Steps

Step	Action
1	Enter the <code>no stack-monitor</code> command to disable stack monitoring.
2	Observe the command output.

---

—End—

---

## Network monitoring configuration using Device Manager

This chapter describes how to use Device Manager to configure system logging and to display chassis and port statistics for the Ethernet Routing Switch 2500 Series.

### Navigation

- "CPU and memory utilization" (page 29)
- "Viewing the system log settings " (page 30)
- "Viewing the Remote System Log tab" (page 32)
- "Graphing chassis statistics" (page 33)
- "Graphing port statistics" (page 41)
- "Configuring the stack monitor " (page 47)

### CPU and memory utilization

Use this procedure to view both CPU and memory utilization.

#### Procedure Steps

Step	Action
1	Navigate to <b>Edit, Chassis</b>
2	Select the <b>CPU/Mem Utilization</b> tab
3	Click the <b>Refresh</b> 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.
MemoryTotalMB	Total memory present, in megabytes, on the unit.
MemoryAvailableMB	Memory remaining available on the unit.

## Viewing the system log settings

Use this procedure to view System Log Settings information.

### Procedure Steps

Step	Action
1	From the Device Manager menu bar, select <b>Edit, Diagnostics, System Log</b> .
2	Select the <b>System Log Settings</b> tab if it is not already displayed.
—End—	

### Job aid

The following table describes the System Log Settings fields.

Field	Description
Operation	<p>Enables you to store or discard generated log messages.</p> <p>Specifying on stores log messages in the log message buffer facility according to the parameters specified by related management objects. Specifying off discontinues log message accumulation.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="text-align: center;"><b>ATTENTION</b></p> <p>This does not affect operation of the remote syslog facility, it only determines whether log messages are stored locally.</p> </div>
BufferFullAction	<p>Specifies the action to take when buffer space is exhausted.</p> <p>Overwrite causes the previous messages to be overwritten. Messages are overwritten based on First In First Out (FIFO). Specifying latch causes no more messages to be saved until this object is changed to overwrite or until the buffer space is made available through some other means (for example, clearing the buffer).</p>
Volatile—CurSize	<p>Displays the current number of log messages in the volatile portion of the system log message facility. Messages that are classified as volatile are lost upon system reinitialization.</p>
Volatile—SaveTargets	<p>Determines the type of log messages that are saved in the log message buffer facilities. Messages are classified based on their type.</p> <p>Selecting the type - Critical(1), Serious(2), or Informational(3), causes all log messages with an associated value less than or equal to the type value specified to be saved when the log message is entered into the system.</p> <p>For example, specifying the value Critical(1) causes only messages classified as critical to be saved to nonvolatile storage. Specifying Serious(2)</p>

Field	Description
	causes critical and serious messages to be saved. Specifying a value of None(4) means no log messages are stored in volatile memory.
non-Volatile—CurSize	Displays the current number of log messages that are present in the nonvolatile portion of the system log message facility.  Messages that are classified as nonvolatile are saved across system reinitializations.
non-Volatile—SaveTargets	Determines the type of log messages that are saved to nonvolatile storage when they occur. Messages are classified based on their type.  Selecting a type value causes all log messages with an associated value less than or equal to the type value specified to be saved when the log message is entered into the system.  For example, specifying the value Critical(1) causes only messages classified as critical to be saved to nonvolatile storage. Specifying Serious(2) causes critical and serious messages to be saved. Specifying None(4) causes no messages to be saved.
ClearMessageBuffers	Indicates that the messages currently saved in the log message buffer are to be deleted. All messages of types matching the specified bits are deleted. For example, specifying volInformational deletes all informational messages and specifying nonVolCritical deletes all critical messages from nonvolatile storage.

## Viewing the Remote System Log tab

Use this procedure to view Remote System Log information.

### Procedure Steps

Step	Action
1	From the Device Manager menu bar, select <b>Edit, Diagnostics, System Log</b> .
2	Click the <b>Remote System Log</b> tab.
—End—	



**Job aid**

The following table describes the Remote System Log tab fields.

Field	Description
Address	Specifies the IP address of the remote system.
Enabled	Determines whether remote logging is enabled or disabled.
SaveTargets	<p>Determines the type of log messages that are saved in the log message buffer facilities. Messages are classified based on their type.</p> <p>Selecting a type of critical, critical/serious, or critical/serious/inform causes all log messages with the type value specified to be saved when the log message is entered into the system.</p> <p>For example, specifying the value critical causes only messages classified as critical to be sent to the remote system. Specifying critical/serious causes critical and serious messages to be saved. Specifying a value of none means no log messages are sent to the remote system.</p>

**Graphing chassis statistics**

Use the following procedure to graph chassis statistics

**Procedure Steps**

Step	Action
1	From the Device Manager main menu, select <b>Edit, Select, Chassis</b> .
2	Do one of the following: <ul style="list-style-type: none"> <li>From the Device Manager main menu, select <b>Graph, Chassis</b>.</li> <li>From the toolbar, select <b>Graph Selected</b>.</li> </ul>
—End—	

The following sections contains information about the Graph Chassis dialog box tabs with descriptions of the statistics on each tab.

- ["Viewing IP statistics" \(page 34\)](#)

- "Viewing ICMP In statistics" (page 36)
- "Viewing ICMP Out statistics" (page 37)
- "Viewing TCP statistics" (page 38)
- "Viewing UDP statistics" (page 40)

For more information about the **SNMP** tab, see *Nortel Ethernet Routing Switch 2500 Series Security — Configuration and Management* (NN47215-505).

### Viewing IP statistics

Use this procedure to view the IP tab.

---

Step	Action
------	--------

---

1	Select <b>Edit, Select, Chassis</b> .
---	---------------------------------------

2	Do one of the following:
---	--------------------------

- From Device Manager main menu, select **Graph, Chassis**.
- On the toolbar, click **Graph**.

The **Chassis** dialog box appears with the **SNMP** tab displayed.

3	Click the <b>IP</b> tab.
---	--------------------------

The IP tab appears.

---

—End—

---

### Job aid

The following table describes the Chassis 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.

Field	Description
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 Source-Routed by way of this address with successful Source-Route option processing.
InUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InDiscards	The number of input IP datagrams for which no problems are encountered to prevent their continued processing, but that are discarded (for example, for lack of buffer space). Note that 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. Note that this counter does not include any datagrams counted in ipForwDatagrams.
OutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that are discarded (for example, for lack of buffer space). Note that this counter can include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
OutNoRoutes	The number of IP datagrams discarded because no route can be found to transmit them to their destination. Note that this counter also includes any packets counted in ipForwDatagrams that have no route. Note that this includes any datagrams a host cannot route because all of its default gateways are down.
FragOKs	The number of IP datagrams successfully fragmented at this entity.

Field	Description
FragFails	The number of IP datagrams that are discarded because they need to be fragmented at this entity but cannot be, for example, because their Don't Fragment flag was set.
FragCreates	The number of generated IP datagram fragments because of a fragmentation at this entity.
ReasmReqds	The number of IP fragments received that needed to be reassembled at this entity.
ReasmOKs	The number of IP datagrams successfully reassembled.
ReasmFails	The number of failures detected by the IP reassembly algorithm (for example, timed out, errors). Note that 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 ICMP In statistics

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

#### Procedure Steps

Step	Action
1	From the Device Manager main menu, select <b>Edit, Select, Chassis</b> .
2	Do one of the following: <ul style="list-style-type: none"> <li>From Device Manager main menu, select <b>Graph, Chassis</b>.</li> <li>On the toolbar, click <b>Graph</b>.</li> </ul> <p>The Chassis dialog box appears with the SNMP tab displayed.</p>
3	Click <b>ICMP In</b> . The ICMP In tab appears.

—End—

### Job aid

The following table describes the ICMP In tab fields.

Field	Description
SrcQuenchs	The number of ICMP Source Quench messages received.
Redirects	The number of ICMP Redirect messages received.

Field	Description
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 ICMP Out statistics

The chassis ICMP Out shows ICMP Out statistics.

To open the ICMP Out tab, use the following procedure:

Step	Action
1	From the Device Manager main menu, select <b>Edit, Select, Chassis</b> .
2	Do one of the following: <ul style="list-style-type: none"> <li>From Device Manager main menu, select <b>Graph, Chassis</b>.</li> <li>On the toolbar, click <b>Graph</b>.</li> </ul> <p>The Chassis dialog box appears with the SNMP tab displayed.</p>
3	Click <b>ICMP Out</b> . The ICMP Out tab appears.

—End—

### ICMP Out tab fields

The following table describes the ICMP Out tab fields.

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

### Viewing TCP statistics

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

#### Procedure Steps

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | From the Device Manager main menu, select <b>Edit, Select, Chassis</b> .   |
| 2 | Do one of the following: <ul style="list-style-type: none"> <li>From Device Manager main menu, select <b>Graph, Chassis</b>.</li> <li>On the toolbar, click <b>Graph</b>.</li> </ul> |

The Chassis dialog box appears with the SNMP tab displayed.

- |   |  |
|---|--|
| 3 | Click <b>TCP</b> .<br>The TCP tab appears. |
|---|--|

---

—End—

---

**Job aid**

The following table details the fields in the TCP tab.

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

## Viewing UDP statistics

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

### Procedure Steps

Step	Action
1	From the Device Manager main menu, select <b>Edit, Select, Chassis</b> .
2	Do one of the following: <ul style="list-style-type: none"> <li>From Device Manager main menu, select <b>Graph, Chassis</b>.</li> <li>On the toolbar, click <b>Graph</b>.</li> </ul> <p>The <b>Chassis</b> dialog box appears with the <b>SNMP</b> tab displayed.</p>
3	Click <b>UDP</b> . The <b>UDP</b> tab appears.

—End—

### Job aid

The following table details the fields on the UDP tab.

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



## Graphing port statistics

You can graph the following statistics for either a single port or multiple ports from the graphPort dialog box:

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

The windows that appear when you configure a single port differ from the ones appearing when you configure multiple ports. However, the options are similar.

The figures in this section show graphs for multiple ports.

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

### Procedure Steps

Step	Action
1	Select the port or ports you want to graph.  To select multiple ports, press <b>Ctrl+left-click</b> the ports that you want to configure. A yellow outline appears around the selected ports.
2	Do one of the following: <ul style="list-style-type: none"> <li>• From the Device Manager main menu, select <b>Graph, Port</b>.</li> <li>• From the shortcut menu, select <b>Graph</b>.</li> <li>• On the toolbar, click <b>Graph</b>.</li> </ul>
—End—	

The graphPort dialog box for a single port or for multiple ports appears with the Interface tab displayed.

#### ATTENTION

Some statistics are only available when you graph a single port.

### Graphing the Interface tab

The Interface tab shows interface parameters for graphing a port or ports.

Use the following procedure to open the Interface tab for graphing.

### Procedure Steps

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | <p>Select a single or multiple ports you want to graph.</p> <p>To select multiple ports, press <b>Ctrl+left-click</b> the ports that you want to configure. A yellow outline appears around the selected ports.</p>                                |
| 2 | <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>From the Device Manager main menu, select <b>Graph, Port</b>.</li> <li>From the shortcut menu, select <b>Graph</b>.</li> <li>On the toolbar, click <b>Graph</b>.</li> </ul> |

The Port dialog box for a single port or for multiple ports appears with the Interface tab displayed.

—End—

### Job aid

The following table describes the Interface tab fields for graphing ports.

Field	Description
InOctets	The total number of octets received on the interface, including framing characters.
OutOctets	The total number of octets transmitted out of the interface, including framing characters.
InUcastPkts	The number of packets delivered by this sublayer to a higher sublayer that are not addressed to a multicast or broadcast address at this sublayer.
OutNUcastPkts	The total number of packets that higher-level protocols requested be transmitted, and that are addressed to a multicast or broadcast address at this sublayer, including those that are discarded or not sent.
InDiscards	The number of inbound packets chosen to be discarded even though no errors were detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet can be to free up buffer space.

Field	Description
OutDiscards	The number of outbound packets chosen to be discarded even though no errors were detected to prevent their being transmitted. One possible reason for discarding such a packet can be to free up buffer space.
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 cannot be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that cannot be transmitted because of errors.
InUnknownProtos	For packet-oriented interfaces, the number of packets received via the interface that are discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received via the interface that are discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter is always zero.
InMulticastPkts	The number of packets delivered by this sublayer to a higher sublayer that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both group and functional addresses.
OutMulticastPkts	The number of packets that higher-level protocols requested be transmitted, and that are addressed to a multicast address at this sublayer, including those that were discarded or not sent. For a MAC layer protocol, this number includes both group and functional addresses.
InBroadcastPkts	The number of packets delivered by this sublayer to a higher sublayer that are addressed to a broadcast address at this sublayer.
OutBroadcastPkts	The number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this sublayer, including those that were discarded or not sent.

## Graphing the Ethernet Errors tab

The Ethernet Errors tab shows port Ethernet Errors statistics.

Use the following procedure to open the Ethernet Errors tab for graphing,

### Procedure Steps

Step	Action
1	Select the port or ports you want to graph. To select multiple ports, press <b>Ctrl+left-click</b> the ports that you want to configure. A yellow outline appears around the selected ports.
2	Do one of the following: <ul style="list-style-type: none"> <li>From the Device Manager main menu, select <b>Graph, Port</b>.</li> <li>From the shortcut menu, select <b>Graph</b>.</li> <li>On the toolbar, click <b>Graph</b>.</li> </ul> The Graph Port dialog box for a single port or for multiple ports appears with the Interface tab displayed.
3	Click <b>Ethernet Errors</b> . The Ethernet Errors tab appears.



—End—

### Job aid

The following table describes the 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 when the AlignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.

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

Field	Description
SQETestErrors	A count of times that the SQE Test Errors message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
Deferred Transmissions	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.
SingleCollision Frames	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.
MultipleCollision Frames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	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.

### Misc. Stats tab

The Misc. Stats tab shows miscellaneous port statistics.

Use the following procedure to open the Misc. Stats tab for graphing.

### Procedure Steps

Step	Action
1	Select the port or ports you want to graph.

- 2 From the Device Manager main menu, select **Graph, Port**.  
The **Graph Port** dialog box appears with the **Interface** tab displayed.
- 3 Click **Misc. Stats**.  
The Misc. Stats tab appears.

---

—End—

---

### Job aid

The following table describes the Misc. Stats tab fields.

Field	Description
NoResources PktsDropped	The number of packets dropped due to switch memory shortage.

## Configuring the stack monitor

Use this procedure to configure stack monitor parameters with DM.

### Procedure Steps

Step	Action
1	Select <b>Edit, Chassis</b> in DM
2	Select the <b>Stack Monitor</b> tab.
3	Input the required parameters.
4	Click <b>Apply</b> to apply new settings.

---

—End—

---

### Job aid

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

Parameter	Description
StackErrorNotificationEnabled	Enable or disable stack monitoring.
ExpectedStackSize	Set stack size to be monitored in the range of 2 to 8.
StackErrorNotificationInterval	Set interval between traps in the range of 30 to 300 Seconds.





---

## Network monitoring configuration using Web-based management

---

This chapter describes how you can configure network monitoring features using web-based management.

### Navigation

- ["CPU and memory utilization" \(page 49\)](#)
- ["Using the trap Web page to identify trap receivers" \(page 49\)](#)
- ["Viewing the system log" \(page 51\)](#)
- ["Configuring port mirroring" \(page 52\)](#)
- ["Viewing statistics" \(page 53\)](#)
- ["Monitoring MLT traffic" \(page 60\)](#)

### CPU and memory utilization

Use this procedure to view both CPU and memory utilization.

#### Procedure Steps

Step	Action
1	Navigate to <b>Administration, CPU / Memory Utilization</b>
2	Observe the information displayed.
—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 <b>Configuration, SNMP Trap</b> to view the SNMP trap page.
2	In the <b>Trap Web Page</b> area, select the trap receiver you wish to view.
3	Enable or disable the traps as required.
4	Click the <b>Submit</b> button.

—End—

### Stack Health

Use this procedure to view stack health information.

#### Procedure Steps

Step	Action
1	Navigate to <b>Summary, Stack Health</b>
2	Observe the information displayed.

—End—

### Job Aid

The following table describes the fields on the Stack Health Web page, Stack Links section.

Field	Description
Unit	Unit number in the stack.
Description	Description of the unit.
Cascade Up	Status of the stacking connection for the up link.
Cascade Down	Status of the stacking connection for the down link.
Stack Role	Identifies the role of the unit. In the case of a base unit, the field will display <i>base</i>

The following table describes the fields on the Stack Health Web page, Diagnosis section.

Field	Description
Stack Units Found	Total number of units found in the stack.
Stack Health Check	Health check for the stack.
Stack Diagnosis	Description of the stack health.

## Viewing the system log

You can view a display of messages in Nonvolatile Random Access Memory (NVRAM) or Dynamic Random Access Memory (DRAM) and NVRAM.

Use the following procedure to open the System Log page.

Step	Action
1	From the main menu, select <b>Fault, System Log</b> . The System Log page appears.
2	In the <b>System Log (View By)</b> section do one or more of the following: <ul style="list-style-type: none"> <li>select where you want to display messages.</li> <li>select to clear messages from Volatile or Non Volatile memory.</li> </ul>
3	Click <b>Submit</b> . The results of your request are displayed in the System Log section.
—End—	

## Job Aid

The following table describes the fields on the System Log page.

Section	Field	Range	Description
System Log (View By)	Display Messages From	(1) Non Volatile (2) Volatile + Non Volatile	Choose to display messages from NVRAM or DRAM and Non Volatile memory.  The default setting is Non Volatile.
	Clear Messages From	(1) Volatile (2) Volatile + Non Volatile	Choose to clear messages from Volatile memory or Volatile and Non Volatile memory.

Section	Field	Range	Description
		(3) None	If you clear Volatile messages, existing Non Volatile messages are copied into Volatile memory. After a system reset, all existing Non Volatile messages are also copied to Volatile memory. The default settings is None (does not clear messages).
System Log	Index		The number of the event.
	Time Stamp		The time, in hundredths of a second, between system initialization and the time the log messages entered the system.
	Message Type		The type of message. The options are Critical (1), Serious (2), and Informational (3).
	Message		A character string that identifies the origin of the message and the reason why the message was generated.

## Configuring port mirroring

The Ethernet Routing Switch 2500 Series supports port mirroring to analyze traffic. You can view existing port mirroring activity and configure a specific switch port to mirror one specified port.

Use this procedure to configure port mirroring.

### Procedure Steps

Step	Action
1	From the main menu, select <b>Applications, Port Mirroring</b> . The Port Mirroring page appears.
2	Type information in the text boxes, or select from a list.
3	Click <b>Submit</b> .
—End—	

**Job aid**

The following table describes the items on the Port Mirroring page.

Item	Range	Description
Monitoring Mode	Disabled --> Port X Port X --> <--> Port X	The default setting is Disabled. Monitor all traffic received by Port X. Monitor all traffic transmitted by Port X. Monitor all traffic received and transmitted by Port X.
Monitor Port	1..52	Choose the switch port to designate as the monitor port.
Port X	1..52	Choose the switch port to be monitored by the designated monitor port. This port is monitored according to the value X in the Monitoring Mode field.

**Viewing statistics**

This section describes the use of Web-based management to monitor system statistical data.

- ["Viewing port statistics" \(page 53\)](#)
- ["Viewing interface statistics" \(page 57\)](#)
- ["Viewing Ethernet error statistics" \(page 58\)](#)
- ["Viewing transparent bridging statistics" \(page 59\)](#)
- ["Viewing port statistics" \(page 53\)](#)
- ["Viewing interface statistics" \(page 57\)](#)
- ["Viewing Ethernet error statistics" \(page 58\)](#)
- ["Viewing transparent bridging statistics" \(page 59\)](#)

**Viewing port statistics**

You can view detailed statistics about a selected switch port. Both received and transmitted statistics are displayed so that you can compare throughput or other port parameters.

Use the following procedure to view statistical data about a selected switch port.

**Procedure Steps****Step Action**

- 1 From the main menu, select **Statistics, Port**.  
The **Port** page appears. .

- 2 In the **Port Statistics** section, select the port number.
- 3 Click **Submit**.  
The **Port Statistics Table** is updated with information about the selected device and port.
- 4 To update the statistical information, click **Update**.

---

—End—

---

### Job aid

The following table describes the items on the Port page, Port Statistics (View By) section.

Item	Description
Port	The switch port number to monitor.

The following table describes the items on the Port page, Port Statistic Table section.

Item	Description
Packets	The number of packets received and transmitted on this port, including bad packets, broadcast packets, and multicast packets.
Multicasts	The number of good multicast packets received and transmitted on this port, excluding broadcast packets.
Broadcasts	The number of good broadcast packets received and transmitted on this port.
Total Octets	The number of octets of data received and transmitted on this port, including data in bad packets and FCS octets, and framing bits.
Pause Frames	The number of pause frames received and transmitted on this port. Pause frames cause the transmitting port to temporarily suspend the transmission of packets when the receiving port's frame buffer is full (gigabit ports only).
FCS/Frame Errors	The number of valid-size packets received on this port with proper framing but discarded because of FCS Errors.

Item	Description
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 are received on this port with proper CRC and framing that meet the following requirements: <ul style="list-style-type: none"> <li>• 1518 bytes if no VLAN tag exists</li> <li>• 1522 bytes if a VLAN tag exists</li> </ul>
Filtered Packets	The number of packets that are received on this port and discarded because of the specific configuration. This counter does not count the FCS or Frames error packets. This counter counts packets discarded because STP is not set to forwarding, the frame setting in VLAN directs discarding, or there is a mismatch in ingress or egress port speeds.
Frame Errors	The number of valid-size packets received on this port with proper framing but discarded because of Frame Errors.
Collisions	The number of collisions detected on this port.
Single Collisions	The number of packets that are transmitted successfully on this port after a single collision.
Multiple Collisions	The number of packets that are transmitted successfully on this port after more than one collision.
Excessive Collisions	The number of packets lost on this port due to excessive collisions.
Deferred Packets	The number of frames that are delayed on the first transmission attempt, but never incurred a collision.
Late Collisions	The number of packets collisions that occurred after a total length of time that exceeded 512 bit-times of packet transmission.

The following table describes the items on the Port page, Packets Received and Transmitted section.

Item	Description
64 bytes	The number of packets this size received and transmitted successfully on this port.

Item	Description
65-127 bytes	The number of packets this size received and transmitted successfully on this port.
128-255 bytes	The number of packets this size received and transmitted successfully on this port.
256-511 bytes	The number of packets this size received and transmitted successfully on this port.
512-1023 bytes	The number of packets this size received and transmitted successfully on this port.
1024-1518 bytes	The number of packets this size received and transmitted successfully on this port.
1522- 9216 bytes (Jumbo)	The number of packets this size received and transmitted successfully on this port.

### Zeroing ports

Use the following procedure to clear the statistical information for a specific port.

#### Procedure Steps

Step	Action
1	From the main menu, select <b>Statistics, Port</b> . The <b>Port</b> page appears. .
2	In the <b>Port Statistics</b> section, select the port number.
3	Select the <b>Zero Port</b> button to zero the data on the port.
—End—	



### Zeroing all ports

Use the following procedure to clear the statistical information for all ports.

#### Procedure Steps

Step	Action
1	From the main menu, select <b>Statistics, Port</b> . The <b>Port</b> page appears. .
2	In the <b>Port Statistics</b> section, select the port number.
3	Select the <b>Zero All Ports</b> button to zero all the data on all ports.



---

—End—

---

## Viewing interface statistics

You can view selected switch interface statistics.

Use this procedure to view an interface's statistical information.

### Procedure steps

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | From the main menu, select <b>Statistics, Interface</b> .<br>The Interface page appears. |
| 2 | To update the statistical information, select the <b>Update</b> button.                  |

---

—End—

---

### Job aid

The following table describes the Interface page items.

Item	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 are 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 are discarded or not sent.

Item	Description
In Discards	The number of inbound packets that 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 that 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 Protocols	The number of packets received through the interface that were discards due to an unknown or unsupported protocol.

### Viewing Ethernet error statistics

You can view Ethernet error statistics for each monitored interface linked to the Ethernet Routing Switch 2500 Series.

Use the following procedure to view Ethernet error statistics.

#### Procedure Steps

Step	Action
1	From the main menu, select <b>Statistics, Ethernet Errors</b> . The <b>Ethernet Errors</b> page appears. .
2	To refresh the statistical information, click <b>Update</b> .
—End—	

#### Job aid

The following table describes the Ethernet Errors page items.

Item	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.

Item	Description
Internal MAC Transmit Errors	The number of frames for which transmission on a particular interface fails due to 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 due to 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 were lost or never asserted when attempting to transmit a frame on a particular interface.
SQE Test Errors	The number of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985, and its generation is described in section 7.2.4.6 of the same document.
Deferred Transmissions	The number of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.
Single Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
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

You can view the transparent bridging statistics measured for each monitored interface on the device.

Use this procedure to view transparent bridging statistics.

Step	Action
1	From the main menu, select <b>Statistics, Transparent Bridging</b> . The <b>Transparent Bridging</b> page appears.
2	To refresh the statistical information, click <b>Update</b> .
—End—	

### Job aid

The following table describes the Transparent Bridging page items.

Item	Description
Port	The port number that corresponds to the selected switch.
InFrames	The number of frames this port receives 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.
OutFrames	The number of frames this port transmits 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.
InDiscards	The number of valid frames received which were discarded by the forwarding process.

## Monitoring MLT traffic

You can monitor the bandwidth usage for the MultiLink Trunk member ports within each trunk in your configuration by selecting the traffic type to monitor.

Use this procedure to monitor MultiLink Trunk traffic.

### Procedure Steps

Step	Action
1	From the main menu, select <b>Applications, MultiLink Trunk, Utilization</b> . The <b>Utilization</b> page appears.

2 In the MultiLink Trunk Utilization Selection section, type the Trunk number and traffic type to be monitored.

3 Click **Submit**.

The results of your request are displayed in the MultiLink Trunk Utilization Table. .

---

—End—

---

### Job aid

The following table describes the Utilization page items.

Section	Item	Range	Description
MultiLink Trunk Utilization Selection (View By)	Trunk	1..6	Choose the trunk to be monitored.
	Traffic Type	(1) RX and TX (2) RX (3) TX	Choose the traffic type to be monitored for percentage of bandwidth utilization.
MultiLink Trunk Utilization Table	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.



## RMON using the NNCLI

This section describes the CLI commands used to configure and manage RMON. For details see the following section:

- "Viewing the RMON alarms" (page 63)
- "Viewing the RMON events" (page 64)
- "Viewing the RMON history" (page 64)
- "Viewing the RMON statistics" (page 64)
- "Configuring RMON alarms" (page 65)
- "Deleting RMON alarms" (page 66)
- "Configuring RMON events settings" (page 66)
- "Deleting RMON events settings" (page 67)
- "Configuring RMON history settings" (page 67)
- "Deleting RMON history settings" (page 68)
- "Configuring RMON statistics settings" (page 69)
- "Deleting RMON statistics " (page 69)

### Viewing the RMON alarms

Use this procedure to display information about RMON alarms.

#### Procedure Steps

Step	Action
1	Enter Global Configuration mode
2	Enter the <code>show rmon alarm</code> command.
3	Observe the NNCLI output.
—End—	

## Viewing the RMON events

Use this procedure to display information about RMON events.

### Procedure Steps

Step	Action
1	Enter Global Configuration mode
2	Enter the <code>show rmon event</code> command.
3	Observe the NNCLI output.
—End—	

## Viewing the RMON history

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

### Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the <code>show rmon history</code> command.
3	Observe the NNCLI output.
—End—	

## Viewing the RMON statistics

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

### Procedure Steps

Step	Action
1	Enter Global Configuration mode
2	Enter the <code>show rmon stats</code> command.
3	Observe the NNCLI output.
—End—	



## Configuring RMON alarms

Use this procedure to set RMON alarms and thresholds.

### Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the <code>rmon alarm</code> <code>&lt;1-65535&gt;</code> <code>&lt;WORD&gt;</code> <code>&lt;1-2147483647&gt;</code> <code>{absolute   delta}</code> <code>rising-threshold</code> <code>&lt;-2147483648-2147483647&gt;</code> <code>[&lt;1-65535&gt;]</code> <code>falling-threshold</code> <code>&lt;-2147483648-2147483647&gt;</code> <code>[&lt;1-65535&gt;]</code> <code>[owner &lt;LINE&gt;]</code> command.
3	Observe the NNCLI output.
—End—	

### Variable Definitions

The following table describes the parameters for this command.

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

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

## Deleting RMON alarms

Use this procedure to delete RMON alarm table entries. When the variable is omitted, all entries in the table are cleared.

### Deleting the RMON alarms using NNCLI

Step	Action
1	Enter Global Configuration mode.
2	Enter the <code>no rmon alarm [&lt;1-65535&gt;]</code> command.
3	Observe the NNCLI output.
—End—	

### Variable Definitions

The following table describes the command parameters.

Variable	Definition
<1-65535>	Unique identifier of the alarm.

## Configuring RMON events settings

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

### Procedure Steps

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

---

—End—

---

### Variable Definitions

The following table describes the command parameters

Variable	Definition
<1-65535>	Unique index for the event entry.
[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 events settings

Use this procedure to delete RMON event table entries. When the variable is omitted, all entries in the table are cleared.

#### Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the <code>no rmon alarm [&lt;1-65535&gt;]</code> command.
3	Observe the NNCLI output.
—End—	

### Variable Definitions

The following table describes the command parameters.

Variable	Definition
<1-65535>	Unique identifier of the alarm.

### Configuring RMON history settings

Use this procedure to configure RMON history settings.

**Procedure Steps**

Step	Action
1	Enter Global Configuration mode.
2	Enter the <code>rmon history &lt;1-65535&gt; &lt;LINE&gt; &lt;1-65535&gt; &lt;1-3600&gt; [owner &lt;LINE&gt;]</code> command.
3	Observe the NNCLI output.
—End—	

**Variable Definitions**

The following table describes the command parameters.

Variable	Definiton
<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 settings**

Use this procedure to delete RMON history table entries.

**Procedure Steps**

Step	Action
1	Enter Global Configuration mode.
2	Enter the <code>no rmon history [&lt;1-65535&gt;]</code> command.
3	Observe the NNCLI output.
—End—	

**Variable Definitions**

The following table describes the command parameters.

Variable	Definition
<1-65535>	Unique identifier of the alarm.

## Configuring RMON statistics settings

Use this procedure to configure RMON statistics settings.

### Configuring RMON statistics settings using NNCLI

Step	Action
1	Enter Global Configuration mode.
2	Enter the <code>rmon stats &lt;1-65535&gt; &lt;LINE&gt; [owner &lt;LINE&gt;]</code> command.
3	Observe the NNCLI output.
—End—	

Run the `rmon stats` command in Global Configuration command mode.

### Variable Definition

The following table describes the command parameters.

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

## Deleting RMON statistics

Use this procedure to disable RMON statistics. When the variable is omitted, all entries in the table are cleared.

### Procedure Steps

Step	Action
1	Enter Global Configuration mode.
2	Enter the <code>no rmon stats [&lt;1-65535&gt;]</code> command.
3	Observe the NNCLI output.
—End—	

### Variable Definitions

The following table describes the command parameters.

Variable	Definition
<1-65535>	Unique identifier of the alarm.

---

## RMON using Device Manager

---

The Remote Network Monitoring (RMON) MIB is an interface between the RMON agent on an Ethernet Routing Switch 2500 Series and an RMON management application, such as the Device Manager.

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

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

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

### Navigation

- ["Working with RMON information" \(page 71\)](#)
- ["Creating an alarm" \(page 79\)](#)
- ["Deleting an alarm" \(page 81\)](#)
- ["Viewing RMON statistics and history" \(page 82\)](#)
- ["Using RMON events" \(page 84\)](#)
- ["Viewing RMON log information" \(page 86\)](#)

### Working with RMON information

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

#### Viewing statistics

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

Use the following procedure to view RMON Ethernet statistics.

### Procedure Steps

Step	Action
1	Select an object (port).
2	Do one of the following: <ul style="list-style-type: none"> <li>From the shortcut menu, select <b>Graph</b>.</li> <li>From the Device Manager main menu, select <b>Graph, Port</b>.</li> </ul> <p>The Graph Port dialog box appears with the Interface tab displayed.</p>
3	Click <b>RMON</b> . The RMON tab appears.






---

—End—

---

### Job aid

The following table describes 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 are directed to the broadcast address. Note that this does not include multicast packets.
MulticastPkts	The total number of good packets received that are directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
CRCAAlignErrors	The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).



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

The following table describes the types of statistics.

Statistic	Description
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 displayed at the bottom of the graph window.
Average/sec	The cumulative count divided by the cumulative elapsed time.
Min/sec	The minimum average for the counter for a given polling interval over the cumulative elapsed time.
Max/sec	The maximum average for the counter for a given polling interval over the cumulative elapsed time.
LastVal/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. However, when the last bucket is reached, bucket 1 is dumped and recycled to hold a new bucket of statistics. Then bucket 2 is dumped, and so forth.

To view RMON history, use the following procedure:

Step	Action
1	From the Device Manager main menu, select <b>RMON, Control</b> .
2	The RMON Control dialog box appears, with the History tab displayed.

—End—

### Creating history items

You can use RMON to collect statistics at intervals. For example, if you want cntRMON statistics to be gathered over the weekend, enough buckets to cover two days is required. To do this, set the history to gather one

bucket each hour, thus covering a 48-hour period. After you set history characteristics, you cannot modify them; you must delete the history and create another one.

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

### Procedure Steps

Step	Action
1	From the Device Manager main menu, select <b>RMON, Control</b> . The RMONControl dialog box appears with the History tab displayed.
2	Click <b>Insert button</b> . The RMONControl, Insert History dialog box appears.
3	Select the port from the port list or type the port number.
4	In the Buckets Requested box, type the number of buckets. The default is <b>50</b> .
5	In the Interval box, type the interval. The default is <b>1800</b> seconds.
6	Type the owner, the network management system that created this entry.
7	Click <b>Insert</b> .

—End—

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

### Job Aid

The following table describes 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.

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

### Disabling history

To disable RMON history on a port, use the following procedure:

Step	Action
1	From the Device Manager main menu, select <b>RMON, Control</b> . The RMONControl dialog box appears with the History tab displayed.
2	Select the row that contains the port ID you want to delete.
3	Click <b>Delete</b> . The entry is removed from the table.

—End—

## Viewing RMON history statistics

Device Manager lets you view RMON history statistics.

To display RMON History statistics, use the following procedure:

---

Step	Action
------	--------

---

- |   |  |
|---|--|
| 1 | In the <b>RMON history</b> tab, select an entry and click <b>Graph</b> . |
| 2 | The <b>RMON history statistics</b> dialog box appears.                   |
- 

—End—

---

## RMON History fields

The following table describes the RMON History fields.

Field	Description
SampleIndex	An index that uniquely identifies the particular sample this entry represents among all the samples associated with the same entry. This index starts at 1 and increases by one as each new sample is taken.
Utilization	The best estimate of the mean physical layer network utilization on this interface during the sampling interval (in hundredths of a percent).
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
BroadcastPkts	The total number of good packets received that are directed to the broadcast address. Note that this does not include multicast packets.
MulticastPkts	The total number of good packets received that are directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
DropEvents	The total number of events in which packets are dropped by the probe due to lack of resources during this sampling. This number is not necessarily the number of packets dropped; it is the number of times this condition has been detected.

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

### Enabling Ethernet statistics gathering

Use this procedure to use RMON to gather Ethernet statistics.

#### Procedure Steps

Step	Action
1	From the Device Manager main menu, select <b>RMON, Control</b> . The RMON Control dialog box appears with the History tab displayed.
2	Click <b>Ether Stats</b> . The <b>Ether Stats</b> tab appears.
<b>Ether Stats tab fields</b> The following table describes the Ether Stats tab fields.	
3	Click <b>Insert</b> . The <b>RMONControl, Insert Ether Stats</b> dialog box appears.
4	Select the port(s). Enter the port number you want or select the port from the list menu . The Device Manager assigns the index.

- 5 Click **OK**.
- 6 Click **Insert**.  
The new Ethernet Statistics entry is displayed in the **Ether Stats** tab.

---

—End—

---

### Job Aid

The following table describes the fields in the Ether Stats 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.
Owner	The network management system which created this entry.

### Disabling Ethernet statistics gathering

Use the following procedure to disable Ethernet statistics that you have set.

Step	Action
1	From the Device Manager main menu, select <b>RMON, Control</b> . The <b>RMONControl</b> dialog box appears with the <b>History</b> tab displayed.
2	Click <b>Ether Stats</b> . The Ether Stats tab appears.
3	Select the row that contains the port ID you want to delete.
4	Click <b>Delete</b> . The <b>Ether Stats</b> entry is removed from the table.

---

—End—

---

### Creating an alarm

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

## Procedure Steps

Step	Action
1	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>From the Device Manager main menu, select <b>RMON, Alarm Manager</b>.</li> <li>On the toolbar, click <b>Alarm Manager</b>.</li> </ul> <p>The <b>Alarm Manager</b> dialog box appears.</p>
2	<p>In the variable field, select a variable for the alarm from the list and a port (or other ID) on which you want to set an alarm.</p> <p>Alarm variables are in three formats:</p> <ul style="list-style-type: none"> <li>A chassis alarm ends in .x where the x index is hard-coded. No further information is required.</li> <li>A card, Spanning Tree Group (STG) or EtherStat alarm ends with a dot (.). You must enter a card number, STG ID, IP address, or EtherStat information.</li> <li>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).</li> </ul> <p>For this example, select Bridge, dot1dStpTopChanges.0 from the variable list. This example is a chassis alarm, indicated by the .0 in the variable.</p> <p>For this example, select Bridge, dot1dStpTopChanges.0 from the variable list. This example is a chassis alarm, indicated by the .0 in the variable.</p>
3	Select a rising and falling value.
4	Select the <b>Insert</b> button.

---

—End—

---

## Job Aid

The following table describes the RMON Insert Alarm dialog box field.



Field	Description	
Variable	<p>Name and type of alarm—indicated by the format:</p> <p><i>alarmname.x</i> where x=0 indicates a chassis alarm.</p> <p><i>alarmname.</i> where the user must specify the index. The 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.</p> <p><i>alarmname</i> with no dot or index is a port-related alarm and results in display of the port selection tool.</p>	
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	When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, the alarm generates a single event.	When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, the alarm generates a single event.
Event Index	Index of the event entry that is used when a rising threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already filled in.)	Index of the event entry that is used when a falling threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already filled in.)

## Deleting an alarm

Use this procedure to delete an alarm

Step	Action
1	From the Device Manager main menu, select <b>RMON, Alarms</b> . The RMONAlarms dialog box appears with the Alarms tab displayed.
2	Select any field for the alarm that you want to delete.
3	Click <b>Delete</b> .
—End—	

## Viewing RMON statistics and history

Use this procedure to view the RMON statistics and history for an alarm you have created.

### Procedure Steps

Step	Action
1	Select the port on which you have created an alarm.
2	From the Device Manager main menu, select <b>RMON, Alarms</b> . The <b>RMONAlarms</b> dialog box appears with the Alarms tab displayed.
—End—	

### Job Aid

The following table describes the RMON Alarms dialog box fields.

Field	Description
Index	Uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device
Interval	The interval in seconds over which data is sampled and compared with the rising and falling thresholds. When setting this variable, note that in the case of deltaValue sampling, you should set the interval short enough so that the sampled variable is unlikely to increase or decrease by 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.

Field	Description
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is <code>absoluteValue(1)</code> , 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 <code>deltaValue(2)</code> , 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 <code>deltaValue</code> , this value is the difference between the samples at the beginning and end of the period. If the sample type is <code>absoluteValue</code> , 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 complete.
StartupAlarm	The alarm that can be sent when this entry is first set to valid. If the first sample after this entry becomes valid is greater than or equal to the <code>risingThreshold</code> and <code>alarmStartupAlarm</code> is equal to <code>risingAlarm(1)</code> or <code>risingOrFallingAlarm(3)</code> , then a single rising alarm is generated. If the first sample after this entry becomes valid is less than or equal to the <code>fallingThreshold</code> and <code>alarmStartupAlarm</code> is equal to <code>fallingAlarm(2)</code> or <code>risingOrFallingAlarm(3)</code> , then a single falling alarm is generated.
RisingThreshold	A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval 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 <code>alarmStartupAlarm</code> is equal to <code>risingAlarm(1)</code> or <code>risingOrFallingAlarm(3)</code> . After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the <code>alarmFallingThreshold</code> .
RisingEventIndex	The index of the <code>eventEntry</code> that is used when a rising threshold is crossed. The <code>eventEntry</code> identified by a particular value of this index is the same as identified by the same value of the <code>eventIndex</code> object. If there is no corresponding entry in the <code>eventTable</code> , then 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. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold and the associated alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3). After a falling event is generated, another such event is not generated until the sampled value rises above this threshold and reaches the alarmRisingThreshold.
FallingEventIndex	The index of the eventEntry that is used when a falling threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable, then no association exists. In particular, if this value is zero, no associated event is generated, because zero is not a valid event index.
Owner	The network management system which created this entry.
Status	The status of this alarm entry.

## Using RMON events

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

### Navigation

- ["Viewing an event" \(page 84\)](#)
- ["Creating an event" \(page 85\)](#)
- ["Deleting an event" \(page 86\)](#)

### Viewing an event

Use this procedure to view a table of events.

#### Procedure Steps

Step	Action
1	From the Device Manager main menu, select <b>RMON, Alarms</b> . The RMONAlarms dialog box appears displaying the Alarms tab.
2	Click <b>Events</b> .

The Events tab appears.

---

—End—

---

### Job aid

The following table describes the RMONAlarms Events tab fields.

Field	Description
Index	This index uniquely identifies an entry in the event table. Each entry defines one event that is to be generated when the appropriate conditions occur.
Description	Specifies whether the event is a rising or a 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 are as follows: <ul style="list-style-type: none"> <li>• none</li> <li>• log</li> <li>• trap</li> <li>• log-and-trap</li> </ul>
Community	The SNMP community string acts as a password. Only those management applications with this community string can view the alarms.
LastTimeSent	The value of sysUpTime at the time this event entry last generated an event. If this entry has not generated any events, this value is zero.
Owner	If traps are specified to be sent to the owner, then this is the name of the machine that receives alarm traps.

### Creating an event

Use this procedure to create an event.

#### Procedure Steps

Step	Action
------	--------

- |   |   |
|---|---|
| 1 | In the RMONAlarms dialog box Events tab, click <b>Insert</b> .<br>The RMONAlarms, Insert Events dialog box appears. |
|---|---|

- 2 . In the Description field, type a name for the event.
- 3 Select the type of event you want.  
You can set the event type to log to save memory or to snmp-trap to reduce traffic from the switch or for better CPU utilization.  
If you select snmp-trap or log-and-trap, you must set trap receivers.
- 4 Click **Insert**.  
The new event is displayed in the Events tab.

---

—End—

---

### Deleting an event

Use this procedure to delete an event.

#### Procedure Steps

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | In the <b>Events</b> tab, select an event <b>Description</b> . |
| 2 | Click <b>Delete</b> .<br>The event is removed from the table.  |

---

—End—

---

### Viewing RMON log information

The Log tab chronicles and describes the alarm activity, which is then generated to viewed.

Use the following procedure to view the Log tab.

#### Procedure Steps

Step	Action
------	--------

- |   |   |
|---|---|
| 1 | From the Device Manager main menu, select <b>RMON, Alarms</b> .<br>The RMONAlarm dialog box appears with the <b>Alarms</b> tab displayed. |
| 2 | Click <b>Log</b> .<br>The Log tab appears.  |

---

—End—

---

**Job aid**

The following table describes the Log tab fields.

Field	Description
Time	The value of sysUpTime when this log entry was created.
Description	An implementation-dependent description of the event that activated the log entry.





---

## RMON using Web-based management

---

The Remote Network Monitoring (RMON) Management Information Base (MIB) is an interface between the RMON agent on a Ethernet Routing Switch 2500 Series and RMON management applications such as the Web-based management user interface. RMON MIB defines objects that are suitable for the management of any type of network. Some groups are specifically targeted for Ethernet networks.

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

### Navigation

- ["Configuring RMON fault threshold parameters" \(page 89\)](#)
- ["Viewing the RMON fault event log" \(page 93\)](#)
- ["Viewing RMON Ethernet statistics" \(page 94\)](#)
- ["Viewing RMON history" \(page 95\)](#)

### Configuring RMON fault threshold parameters

Alarms are useful when you need to know when the value of some variable goes out of range. RMON alarms can be defined on any MIB variable that resolves to an integer value. String variables (such as system description) cannot be used as alarm variables.

#### Navigation

- ["Creating an RMON fault threshold" \(page 89\)](#)
- ["Deleting an RMON threshold configuration" \(page 92\)](#)

#### Creating an RMON fault threshold

You can create the RMON threshold parameters for fault notification (alarms).

**ATTENTION**

RMON threshold configurations are not modifiable. They must be deleted and the information recreated.

Use this procedure to create an RMON threshold.


**Procedure Steps****Step Action**

- 1 From the main menu, select **Fault, RMON Threshold**.  
The RMON Threshold page appears.
- 2 In the RMON Threshold Creation section, type information in the text boxes, or select from a list.
- 3 Click **Submit**.

—End—

**Job aid**

The following table describes the items on the RMON Threshold page.

Item	Range	Description
		Deletes the row.
Index/Event Rising Index/Event Falling Index	1..10	Type the unique number to identify the alarm entry.
Target	Integer	The port number.
Port	1..25	The port on which to set an alarm.
Parameter	(1) Good-Bytes (2) Good-Packets (3) Multicast (4) Broadcast (5) CRC-Errors (6) Runts (7) Fragments (8) Frame-Too-Long (9) Collisions	The sampled statistic.

Item	Range	Description
Current Level	Integer	<p>The value of the statistic during the last sampling period.</p> <div> <p><b>ATTENTION</b></p> <p>If the sample type is delta, the value is the difference between the samples at the beginning and end of the period. If the sample type is Absolute, the value is the sampled value at the end of the period.</p> </div>
Rising Level	Integer	<p>Type the event entry to be used when a rising threshold is crossed.</p> <div> <p><b>ATTENTION</b></p> <p>When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the Falling Threshold.</p> </div>
Rising Action	(1) Log (2) SNMP Trap (3) Log and Trap	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.
Falling Level	Integer	Type the event entry to be used when a Falling Threshold is crossed.

Item	Range	Description
Interval		Type the time period (in seconds) to sample data and compare the data to the rising and falling thresholds.
Sample/Alarm Sample	(1) Absolute (2) Delta	<p>Choose the sampling method.</p> <p><b>Absolute:</b> Absolute alarms are defined on the current value of the alarm variable. An example of an alarm defined with absolute value is card operating status. Because this value is not cumulative, but instead represents states, such as card up (value 1) and card down (value 2), you set it for absolute value. Therefore, an alarm can be created with a rising value of 2 and a falling value of 1 to alert a user to whether the card is up or down.</p> <p><b>Delta:</b> 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 per polling period. For each sample, the last two values are added together and compared to the threshold values. This process increases precision and allows for the detection of threshold crossings that span the sampling boundary. Therefore, if you keep track of the current values of a given delta-valued alarm and add them together, the result is twice the actual value. (This result is not an error in the software.)</p>

### Deleting an RMON threshold configuration

Use this procedure to delete an existing RMON threshold configuration.

#### Procedure Steps

Step	Action
------	--------

- |   |   |
|---|---|
| 1 | <p>From the main menu, select <b>Fault, RMON Threshold</b>.</p> <p>The RMON Threshold page appears.</p> |
|---|---|

- 2 In the RMON Threshold Table, click the **Delete** icon for the entry you want to delete.

A message appears prompting you to confirm your request.

- 3 Do one of the following:
  - Click **Yes** to delete the RMON threshold configuration.
  - Click **Cancel** to return to the RMON Threshold page without making changes.

---

—End—

---

## Viewing the RMON fault event log

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

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

- Rising Event
- Falling Event

Default events specify that when an alarm goes out of range, the firing of the alarm is tracked in both a trap and a log. For example, when an alarm triggers at the rising threshold, the rising event specifies that this information be sent to both a trap and a log. The RMON Event Log page works in conjunction with the RMON Threshold page to enable you to view a history of RMON fault events.

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

### Procedure Steps

---

Step	Action
------	--------

---

- |   |   |
|---|---|
| 1 | From the main menu, select <b>Fault, RMON Event Log</b> . |
| 2 | The RMON Event Log page appears.                          |
- 

—End—

---

**Job aid**

The following table describes the fields on the RMON Event Log page fields.

Field	Description
Time Stamp	The time the event occurred.
Description	An implementation dependent description of the event that activated this log entry.
Triggered By	A comment describing the source of the event.
ID	The event that generated this log entry.

**Viewing RMON Ethernet statistics**

You can gather and graph RMON Ethernet statistics in a variety of formats.

Use this procedure to gather and graph RMON Ethernet statistics.

Step	Action
1	From the main menu, select <b>Statistics, RMON Ethernet</b> . The RMON Ethernet page appears.
2	Click <b>Submit</b> . The RMON Ethernet Statistics Table is updated with information about the selected device. .
—End—	

**Job aid**

The following table describes the items on the RMON Ethernet page.

Item	Description
Port	The port number that corresponds to the selected switch.
Drop Events	The number of events in which packets were dropped by the interface due to a lack of resources.
Octets	The number of octets of data (including those in bad packets) received on the network (excluding framing bits, but including Frame Check Sequence (FCS) octets).
Packets	The number of packets received and transmitted on a port, including bad, broadcast and multicast packets.
Broadcast	The number of good packets received that are directed to the broadcast address. This does not include multicast packets.

Item	Description
Multicast	The number of good packets received that are directed to the multicast address. This does not include packets sent to the broadcast address.
CRC Align Errors	The number of packets received with a length (excluding and 1518 octets, inclusive, but with either a bad Frame FCS with an integral number of octets [FCS errors] with a nonintegral number of octets [alignment error]).
Undersize	The number of packets received that are less than 64 octets long (excluding framing bits, but including FCS octets) and are otherwise well-formed.
Fragments	The number of packets received that are less than 64 octets in length (excluding framing bits, but including FCS octets) and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	The best estimate number of collisions on this Ethernet segment.
Jabbers	The number of packets received that are longer than 1518 octets in length (excluding framing bits, but including FCS octets), and with either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
Packets < = 64 bytes 65-127 bytes 128-255 bytes 256-511 bytes 512-1023 bytes 1024-1518 bytes 1522- 9216 bytes	The number of octets received (including bad packets) in length (excluding framing bits, but including FCS octets).

## Viewing RMON history

You can view a periodic statistical sampling of data from various types of networks.

Use this procedure to view periodic statistical data.

### Procedure Steps

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | From the main menu, select <b>Statistics, RMON History</b> .<br>The RMON History page appears. |
|---|--|

- 2 In the RMON History Statistics section, select the port number to be monitored.
- 3 Click **Submit**.  
The RMON History Statistics Table is updated with information about the selected device and port.

---

—End—

---

### Job aid

The following table describes the items on the RMON History page, Statistics Table (View By) section.

Item	Description
Port	The port number to be monitored.

The following table describes the items on the RMON History page, Statistics Table section.

Item	Description
Start	The value of the sysUptime at the start of the interval over which this sample was measured.
Drop Events	The number of events in which packets were dropped by the interface due to a lack of resources.
Octets	The number of octets of data (including those in bad packets) received on the network (excluding framing bits, but including FCS octets).
Packets	The number of packets received and transmitted on a port, including bad, broadcast and multicast packets.
Broadcast	The number of good packets received that are directed to the broadcast address. This does not include multicast packets.
Multicast	The number of good packets received that are directed to the multicast address. This does not include packets sent to the broadcast address.
CRC Align Errors	The number of packets received with a length between 64 and 1518 octets, but with either a bad Frame FCS with an integral number of octets (FCS errors) with a nonintegral number of octets (alignment error).



Item	Description
Undersize	The number of packets received that are less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
Oversize	The number of packets received that are longer than 1518 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.





Nortel Ethernet Routing Switch 2500 Series

## Configuration — System Monitoring

Copyright © 2007-2008, Nortel Networks  
All Rights Reserved.

Publication: NN47215-502  
Document status: Standard  
Document version: 03.01  
Document date: 27 October 2008

To provide a report a problem in this document, go to [www.nortel.com/feedback](http://www.nortel.com/feedback)

Sourced in Canada, India and the United States of America

The information in this document is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

\*Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

Adobe and Adobe Reader are trademarks of Adobe Systems Incorporated.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

Trademarks are acknowledged with an asterisk (\*) at their first appearance in the document.

All other trademarks are the property of their respective owners.

