This appendix describes the remote monitoring features available on HP products:

### Viewing System Information

You can access software and hardware specifics for an HP Routing Switch.

**USING THE CLI**

To view the software and hardware details for the system, enter the `show version` command:

```
HP9300# show version
```

**Syntax:** `show version`

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Monitor in the tree view to expand the list of monitoring options.
3. Click on the Device link to display the Device Information panel.

### Viewing Configuration Information

You can view a variety of configuration details and statistics with the `show` option. The `show` option provides a convenient way to check configuration changes before saving them to flash.

The show options available will vary by configuration level.

**USING THE CLI**

To determine the available show commands for the system or a specific level of the CLI, enter the following command:

```
HP9300# show ?
```

**Syntax:** `show <option>`

You also can enter “show” at the command prompt, then press the TAB key.

**NOTE:** For a complete summary of all available `show...` CLI commands and their displays, see the *Command Line Interface Reference.*
USING THE WEB MANAGEMENT INTERFACE
1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Monitor in the tree view to expand the list of monitoring options.
3. If needed, click on the plus sign next to a subcategory to display the monitoring links for that category.
4. Click on the link for the information you want to view.

Viewing Port Statistics
Port statistics are polled by default every 10 seconds.

USING THE CLI
You can view statistics for ports by entering the following show commands:
- show interfaces
- show configuration

USING THE WEB MANAGEMENT INTERFACE
To view the port statistics for all ports on a Routing Switch:
1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Monitor in the tree view to expand the list of monitoring options.
3. Click on the plus sign next to Port to expand the list of port monitoring options.
4. Select the Statistic link.

Viewing STP Statistics
You can view a summary of STP statistics for Routing Switches. STP statistics are by default polled every 10 seconds.

To modify this polling rate (when using the Web management interface), select the Preferences link from the main menu, and modify the STP field. You can disable polling by setting the field to zero.

USING THE CLI
To view spanning tree statistics, enter the show span command. To view STP statistics for a VLAN, enter the span vlan command.

USING THE WEB MANAGEMENT INTERFACE
1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Monitor in the tree view to expand the list of monitoring options.
3. Select the STP link.

Clearing Statistics
You can clear statistics for many parameters with the clear option.

USING THE CLI
To determine the available clear commands for the system, enter the following command:
```
HP9300# clear ?
```
**Syntax:** clear <option>
You also can enter “clear” at the command prompt, then press the TAB key.
For a complete summary of all available clear... CLI commands and their displays, see the Command Line Interface Reference.

NOTE: Clear commands are found at the Privileged EXEC level.

USING THE WEB MANAGEMENT INTERFACE

You can clear statistics by doing the following:

1. Log on to the device using a valid user name and password for read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Command in the tree view to expand the list of command options.
3. Click on the Clear link to display the Clear panel.
4. Select all items to be cleared.
5. Click Apply.

RMON Support

The HP RMON agent supports the following groups. The group numbers come from the RMON specification (RFC 1757).

- Statistics (RMON Group 1)
- History (RMON Group 2)
- Alarms (RMON Group 3)
- Events (RMON Group 9)

The CLI allows you to make configuration changes to the control data for these groups, but you need a separate RMON application to view and display the data graphically.

Statistics (RMON Group 1)

Count information on multicast and broadcast packets, total packets sent, undersized and oversized packets, CRC alignment errors, jabbers, collision, fragments and dropped events is collected for each port on an HP Routing Switch.

No configuration is required to activate collection of statistics for the Routing Switch. This activity is by default automatically activated at system start-up.

USING THE CLI

You can view a textual summary of the statistics for all ports by entering the following CLI command:

```
HP9300(config)# show rmon statistics
Ethernet statistics 1 is active, owned by monitor
   Interface 1/1 (ifIndex 1) counters
      Octets          0
      Drop events          0                  Packets          0
      Broadcast pkts          0          Multicast pkts          0
      CRC alignment errors          0          Undersize pkts          0
      Oversize pkts          0                  Fragments          0
      Jabbers          0                Collisions          0
      64 octets pkts          0          65 to 127 octets pkts          0
      128 to 255 octets pkts          0          256 to 511 octets pkts          0
      512 to 1023 octets pkts          0          1024 to 1518 octets pkts          0
```

**Syntax:** show rmon statistics [<portnum>]
The \(<\text{portnum}>\) parameter specifies the port number. You can use the physical port number or the SNMP port number. The physical port number is based on the product.

- The ports are numbered according to slot and port. For example, the first port in slot 1 is 1/1. The third port in slot 7 is 7/3.

The SNMP numbers of the ports start at 1 and increase sequentially. For example, if slot 1 contains an 8-port module, the SNMP number of the first port in slot 2 is 9. The physical port number of the same port is 2/1.

This command shows the following information.

<table>
<thead>
<tr>
<th>This Line...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Octets</td>
<td>The total number of octets of data received on the network. This number includes octets in bad packets. This number does not include framing bits but does include Frame Check Sequence (FCS) octets.</td>
</tr>
<tr>
<td>Drop events</td>
<td>Indicates an overrun at the port. The port logic could not receive the traffic at full line rate and had to drop some packets as a result. The counter indicates the total number of events in which packets were dropped by the RMON probe due to lack of resources. This number is not necessarily the number of packets dropped, but is the number of times an overrun condition has been detected.</td>
</tr>
<tr>
<td>Packets</td>
<td>The total number of packets received. This number includes bad packets, broadcast packets, and multicast packets.</td>
</tr>
<tr>
<td>Broadcast pkts</td>
<td>The total number of good packets received that were directed to the broadcast address. This number does not include multicast packets.</td>
</tr>
<tr>
<td>Multicast pkts</td>
<td>The total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.</td>
</tr>
<tr>
<td>CRC alignment errors</td>
<td>The total number of packets received that were from 64 – 1518 octets long, but 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). The packet length does not include framing bits but does include FCS octets.</td>
</tr>
<tr>
<td>Undersize pkts</td>
<td>The total number of packets received that were less than 64 octets long and were otherwise well formed. This number does not include framing bits but does include FCS octets.</td>
</tr>
</tbody>
</table>
### Table A.1: Export Configuration and Statistics (Continued)

<table>
<thead>
<tr>
<th>This Line...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fragments</strong></td>
<td>The total number of packets received that were less than 64 octets long 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).&lt;br&gt;It is normal for this counter to increment, since it counts both runts (which are normal occurrences due to collisions) and noise hits.&lt;br&gt;This number does not include framing bits but does include FCS octets.</td>
</tr>
<tr>
<td><strong>Oversize packets</strong></td>
<td>The total number of packets received that were longer than 1518 octets and were otherwise well formed.&lt;br&gt;This number does not include framing bits but does include FCS octets.</td>
</tr>
<tr>
<td><strong>Jabbers</strong></td>
<td>The total number of packets received that were longer than 1518 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).&lt;br&gt;<strong>Note:</strong> This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.&lt;br&gt;This number does not include framing bits but does include FCS octets.</td>
</tr>
<tr>
<td><strong>Collisions</strong></td>
<td>The best estimate of the total number of collisions on this Ethernet segment.</td>
</tr>
<tr>
<td><strong>64 octets pkts</strong></td>
<td>The total number of packets received that were 64 octets long.&lt;br&gt;This number includes bad packets.&lt;br&gt;This number does not include framing bits but does include FCS octets.</td>
</tr>
<tr>
<td><strong>65 to 127 octets pkts</strong></td>
<td>The total number of packets received that were 65 – 127 octets long.&lt;br&gt;This number includes bad packets.&lt;br&gt;This number does not include framing bits but does include FCS octets.</td>
</tr>
<tr>
<td><strong>128 to 255 octets pkts</strong></td>
<td>The total number of packets received that were 128 – 255 octets long.&lt;br&gt;This number includes bad packets.&lt;br&gt;This number does not include framing bits but does include FCS octets.</td>
</tr>
<tr>
<td><strong>256 to 511 octets pkts</strong></td>
<td>The total number of packets received that were 256 – 511 octets long.&lt;br&gt;This number includes bad packets.&lt;br&gt;This number does not include framing bits but does include FCS octets.</td>
</tr>
</tbody>
</table>
USING THE WEB MANAGEMENT INTERFACE

To view the RMON statistics for the system:

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration dialog is displayed.
2. Click on the plus sign next to Monitor in the tree view to expand the list of monitoring options.
3. Click on the plus sign next to Port in the tree view to expand the list of Port option links.
4. Click on the Statistics link to display the Port Statistic table.
5. Click on the RMON Ethernet Statistics link to display the RMON Ethernet Statistics table.

The same statistics as those listed for the CLI are displayed.

NOTE: The number of entries in a RMON statistics table directly corresponds to the number of ports on a system. For example, if the system is a 26 port device, there will be 26 entries in the statistics display.

History (RMON Group 2)

All active ports by default will generate two history control data entries per active HP Routing Switch interface. An active port is defined as one with a link up. If the link goes down the two entries are automatically be deleted.

Two history entries are generated for each device:
- a sampling of statistics every 30 seconds
- a sampling of statistics every 30 minutes

The history data can be accessed and displayed using any of the popular RMON applications

USING THE CLI

A sample RMON history command and its syntax is shown below:

HP9300(config)# rmon history 1 interface 1 buckets 10 interval 10 owner nyc02

Syntax: rmon history <entry-number> interface <portnum> buckets <number> interval <sampling-interval> owner <text-string>

You can modify the sampling interval and the bucket (number of entries saved before overwrite) using the CLI. In the above example, owner refers to the RMON station that will request the information.
NOTE: To review the control data entry for each port or interface, enter the `show rmon history` command.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration dialog is displayed.

2. Click on the plus sign next to Monitor in the tree view to expand the list of monitoring options.

3. Click on the plus sign next to Port in the tree view to expand the list of Port option links.

4. Click on the Statistics link to display the Port Statistic table.

5. Click on the History link to display the RMON Ethernet History table.

**Alarm (RMON Group 3)**

Alarm is designed to monitor configured thresholds for any SNMP integer, time tick, gauge or counter MIB object. Using the CLI, you can define what MIB objects are monitored, the type of thresholds that are monitored (falling, rising or both), the value of those thresholds, and the sample type (absolute or delta).

An alarm event is reported each time that a threshold is exceeded. The alarm entry also indicates the action (event) to be taken if the threshold be exceeded.

**USING THE CLI**

A sample CLI alarm entry and its syntax is shown below:

```
HP9300(config)# rmon alarm 1 ifInOctets.6 10 delta rising-threshold 100 1 falling threshold 50 1 owner nyc02
```

**Syntax:** `rmon alarm <entry-number> <MIB-object.interface-num> <sampling-time> <sample-type> <threshold-type> <threshold-value> <event-number> <threshold-type> <threshold-value> <event-number> owner <text-string>`

**USING THE WEB MANAGEMENT INTERFACE**

This display is not supported on the Web management interface.

**Event (RMON Group 9)**

There are two elements to the Event Group—the event control table and the event log table.

The event control table defines the action to be taken when an alarm is reported. Defined events can be found by entering the CLI command, `show event`. The Event Log Table collects and stores reported events for retrieval by an RMON application.

**USING THE CLI**

A sample entry and syntax of the event control table is shown below:

```
HP9300(config)# rmon event 1 description ‘testing a longer string’ log-and-trap public owner nyc02
```

**Syntax:** `rmon event <event-entry> description <text-string> log | trap | log-and-trap owner <rmon-station>`

**USING THE WEB MANAGEMENT INTERFACE**

This display is not supported on the Web management interface.