

## Configuring Real-Time Performance Monitoring (J-Web Procedure)

---

Real-time performance monitoring (RPM) in EX Series switches enables you to configure and send probes to a specified target and monitor the analyzed results to determine packet loss, round-trip time, and jitter. Jitter is the difference in relative transit time between two consecutive probes. You can set up probe owners and configure one or more performance probe tests under each probe owner.

The ways in which you can use RPM include:

- Monitor time delays between devices.
- Monitor time delays at the protocol level.
- Set thresholds to trigger SNMP traps when threshold values are exceeded. You can configure thresholds for round-trip time, ingress or egress delay, standard deviation, jitter, successive lost probes, and total lost probes per test.
- Determine automatically whether a path exists between a host switch and its configured Border Gateway Protocol (BGP) neighbors. You can view the results of the discovery using an SNMP client.
- Use the history of the most recent 50 probes to analyze trends in your network and predict future needs.

Probes collect packets per destination and per application, including PING Internet Control Message Protocol (ICMP) packets, User Datagram Protocol and Transmission Control Protocol (UDP/TCP) packets with user-configured ports, user-configured Differentiated Services code point (DSCP) type-of-service (ToS) packets, and Hypertext Transfer Protocol (HTTP) packets.

EX Series switches support the following tests and probe types:

- Ping tests:
  - ICMP echo
  - ICMP timestamp
- HTTP tests:
  - HTTP get (not available for BGP RPM services)
- UDP and TCP tests with user-configured ports:
  - UDP echo
  - TCP connection
  - UDP timestamp

To account for latency in the communication of probe messages, you can enable timestamping of the probe packets. You should configure both the requester and the responder to timestamp the RPM packets. The RPM features provides an additional configuration option to set one-way hardware timestamps. Use one-way timestamps

when you want information about one-way, rather than round-trip, times for packets to traverse the network between the requester and the responder.



**NOTE:**

- EX Series switches support hardware timestamps for UDP and ICMP probes. EX Series switches do not support hardware timestamps for HTTP or TCP probes.
- If the responder does not support hardware timestamps, RPM can only report the round-trip measurements, it cannot calculate round-trip jitter.
- In EX Series switches timestamps apply only to IPv4 traffic.

To configure RPM using the J-Web interface:

1. Select **Troubleshoot > RPM > Configure RPM** .
2. In the **Configure RPM** page, enter information as specified in Table 1.
  - a. Click **Add** to set up the **Owner Name** and **Performance Probe Tests**.
  - b. Select a probe owner from **Probe Owners** list and click **Delete** to remove the selected probe owner
  - c. Double-click one of the probe owners in **Probe Owners** list to display the list of performance probe tests.
  - d. Double-click one of the performance probe tests to edit the test parameters.
3. Enter the **Maximum Number of Concurrent Probes** and specify the **Probe Servers**.
4. Click **Apply** to apply the RPM probe settings.

**Table 1: RPM Probe Owner, Concurrent Probes, and Probe Servers Configuration Fields**

Field	Function	Your Action
Probe Owners	Identifies a owner for whom one or more RPM tests are configured. In most implementations, the owner name identifies a network on which a set of tests is being run.	<ol style="list-style-type: none"><li>1. Click <b>Add</b> and type an owner name.</li><li>2. In <b>Performance Probe Tests</b>, click <b>Add</b> to define the RPM test parameters. See Table 2 for information on configuring RPM test parameters.</li><li>3. Click <b>OK</b> to save the settings or <b>Cancel</b> to exit from the window without saving the changes.</li></ol>
Maximum Number of Concurrent Probes	Specifies the maximum number of concurrent probes allowed.	Type a number from 1 through 500.

**Table 1: RPM Probe Owner, Concurrent Probes, and Probe Servers Configuration Fields** (continued)

Field	Function	Your Action
Probe Servers	Specifies the servers that act as receivers and transmitters for the probes.	Set up the following servers: <ul style="list-style-type: none"> <li>■ TCP Probe Server—Specifies the port on which the device is to receive and transmit TCP probes. Type the number 7 (a standard TCP port number) or a port number from 49160 through 65535.</li> <li>■ UDP Probe Server—Specifies the port on which the device is to receive and transmit UDP probes. Type the number 7 (a standard TCP port number) or a port number from 49160 through 65535.</li> </ul>

**Table 2: Performance Probe Tests Configuration Fields**

Field	Function	Your Action
<b>Identification</b>		
Test Name	Identifies the RPM test.	Type a test name.
Target (Address or URL)	Specifies the IP address or the URL of the probe target.	Type the IP address in dotted decimal notation or the URL of the probe target. If the target is a URL, type a fully formed URL that includes <code>http://</code> .
Source Address	Specifies the IP address to be used as the probe source address.	Type the source address to be used for the probe. If you do not supply this value, the packet uses the outgoing interface's address as the probe source address.
Routing Instance	Specifies the routing instance over which the probe is sent.	Type the routing instance name. The routing instance applies only to <code>icmp-ping</code> and <code>icmp-ping-timestamp</code> probe types. The default routing instance is <code>inet.0</code> .
History Size	Specifies the number of probe results to be saved in the probe history.	Type a number from 0 through 255. The default history size is 50.
<b>Request Information</b>		
Probe Type	Specifies the type of probe to send as part of the test.	Select a probe type from the list: <ul style="list-style-type: none"> <li>■ <code>http-get</code></li> <li>■ <code>http-get-metadata</code></li> <li>■ <code>icmp-ping</code></li> <li>■ <code>icmp-ping-timestamp</code></li> <li>■ <code>tcp-ping</code></li> <li>■ <code>udp-ping</code></li> <li>■ <code>udp-ping-timestamp</code></li> </ul>

**Table 2: Performance Probe Tests Configuration Fields** (continued)

Field	Function	Your Action
Interval	Sets the wait time (in seconds) between probe transmissions.	Type a number from 1 through 255 .
Test Interval	Sets the wait time (in seconds) between tests.	Type a number from 0 through 86400 .
Probe Count	Sets the total number of probes to be sent for each test.	Type a number from 1 through 15.
Moving Average Size	Specifies the number of samples to be used in the statistical calculation operations to be performed across a number of the most recent samples.	Type a number from 0 through 255.
Destination Port	Specifies the TCP or UDP port to which probes are sent.  To use TCP or UDP probes, you must configure the remote server as a probe receiver. Both the probe server and the remote server must be Juniper Networks network devices configured to receive and transmit RPM probes on the same TCP or UDP port.	Type the number 7 (a standard TCP or UDP port number) or a port number from 49160 through 65535.
DSCP Bits	Specifies the Differentiated Services code point (DSCP) bits. This value must be a valid 6-bit pattern.	Type a valid 6-bit pattern.
Data Size	Specifies the size (in bytes) of the data portion of the ICMP probes.	Type a number from 0 through 65507.
Data Fill	Specifies the hexadecimal value of the data portion of the ICMP probes.	Type a hexadecimal value from 1h through 800h .
<b>Hardware Timestamp</b>		
One Way Hardware Timestamp	Enables one-way hardware timestamp.	To enable timestamping, select the check box.
Destination Interface	Enables hardware timestamp on the specified interface.	Select an interface from the list.
<b>Maximum Probe Thresholds</b>		
Successive Lost Probes	Sets the number of probes that can be lost successively, if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 15.
Lost Probes	Sets the number of probes that can be lost , if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 15.

**Table 2: Performance Probe Tests Configuration Fields** (continued)

Field	Function	Your Action
Round Trip Time	Sets the round-trip time (in microseconds), from the switch to the remote server, if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000.
Jitter	Sets the jitter (in microseconds), if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000.
Standard Deviation	Sets the maximum allowable standard deviation (in microseconds), if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000.
Egress Time	Sets the one-way time (in microseconds), from the switch to the remote server, if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000.
Ingress Time	Sets the one-way time (in microseconds), from the remote server to the switch, if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000 (microseconds).
Jitter Egress Time	Sets the outbound-time jitter (in microseconds), if exceeded triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000.
Jitter Ingress Time	Sets the inbound-time jitter (in microseconds), if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 and 60000000.
Egress Standard Deviation	Sets the maximum allowable standard deviation of outbound times (in microseconds), if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000.
Ingress Standard Deviation	Sets the maximum allowable standard deviation of inbound times (in microseconds), if exceeded, triggers a probe failure and generates a system log message.	Type a number from 0 through 60000000.
<b>Traps</b>		
Egress Jitter Exceeded	Generates SNMP traps when the threshold for jitter in outbound time is exceeded.	<ul style="list-style-type: none"> <li>■ To enable SNMP traps for this condition, select the check box.</li> <li>■ To disable SNMP traps, clear the check box.</li> </ul>

**Table 2: Performance Probe Tests Configuration Fields** (continued)

Field	Function	Your Action
Egress Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in outbound times is exceeded.	<ul style="list-style-type: none"> <li>■ To enable SNMP traps for this condition, select the check box.</li> <li>■ To disable SNMP traps, clear the check box.</li> </ul>
Egress Time Exceeded	Generates SNMP traps when the threshold for maximum outbound time is exceeded.	<ul style="list-style-type: none"> <li>■ To enable SNMP traps for this condition, select the check box.</li> <li>■ To disable SNMP traps, clear the check box.</li> </ul>
Ingress Jitter Exceeded	Generates SNMP traps when the threshold for jitter in inbound time is exceeded.	<ul style="list-style-type: none"> <li>■ To enable SNMP traps for this condition, select the check box.</li> <li>■ To disable SNMP traps, clear the check box.</li> </ul>
Ingress Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in inbound times is exceeded.	<ul style="list-style-type: none"> <li>■ To enable SNMP traps for this condition, select the check box.</li> <li>■ To disable SNMP traps, clear the check box.</li> </ul>
Ingress Time Exceeded	Generates SNMP traps when the threshold for maximum inbound time is exceeded.	<ul style="list-style-type: none"> <li>■ To enable SNMP traps for this condition, select the check box.</li> <li>■ To disable SNMP traps, clear the check box.</li> </ul>
Jitter Exceeded	Generates SNMP traps when the threshold for jitter in round-trip time is exceeded.	<ul style="list-style-type: none"> <li>■ To enable SNMP traps for this condition, select the check box.</li> <li>■ To disable SNMP traps, clear the check box.</li> </ul>
Probe Failure	Generates SNMP traps when the threshold for the number of successive lost probes is exceeded.	<ul style="list-style-type: none"> <li>■ To enable SNMP traps for this condition, select the check box.</li> <li>■ To disable SNMP traps, clear the check box.</li> </ul>
RTT Exceeded	Generates SNMP traps when the threshold for maximum round-trip time is exceeded.	<ul style="list-style-type: none"> <li>■ To enable SNMP traps for this condition, select the check box.</li> <li>■ To disable SNMP traps, clear the check box.</li> </ul>
Standard Deviation Exceeded	Generates SNMP traps when the threshold for standard deviation in round-trip times is exceeded.	<ul style="list-style-type: none"> <li>■ To enable SNMP traps for this condition, select the check box.</li> <li>■ To disable SNMP traps, clear the check box.</li> </ul>
Test Completion	Generates SNMP traps when a test is completed.	<ul style="list-style-type: none"> <li>■ To enable SNMP traps for this condition, select the check box.</li> <li>■ To disable SNMP traps, clear the check box.</li> </ul>

**Table 2: Performance Probe Tests Configuration Fields** (continued)

Field	Function	Your Action
Test Failure	Generates SNMP traps when the threshold for the total number of lost probes is exceeded.	<ul style="list-style-type: none"><li>■ To enable SNMP traps for this condition, select the check box.</li><li>■ To disable SNMP traps, clear the check box.</li></ul>

- Related Topics**
- Configuring SNMP (J-Web Procedure)
  - Viewing Real-Time Performance Monitoring Information

---

Published: 2010-05-03