

Understanding Real-Time Performance Monitoring on EX-series Switches

Real-time performance monitoring (RPM) enables you to configure active probes to track and monitor traffic across the network and investigate network problems. You can use RPM with EX-series switches.

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 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. (SNMP trap results are stored in `pingResultsTable`, `jnxPingResultsTable`, `jnxPingProbeHistoryTable`, and `pingProbeHistoryTable`.)

- Determine automatically whether a path exists between a host router or 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.

RPM provides MIB support with extensions for RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*.

This topic includes:

- RPM Packet Collection on page 1
- Tests and Probe Types on page 1
- Hardware Timestamps on page 2
- Limitations of RPM on page 4

RPM Packet Collection

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.

Tests and Probe Types

A test can contain multiple probes. The probe type specifies the packet and protocol contents of the probe.

EX-series switches support the following tests and probe types:

- Ping tests:
 - ICMP echo probe

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

Hardware Timestamps

To account for latency in the communication of probe messages, you can enable timestamping of the probe packets (hardware timestamps). If hardware timestamps are not configured, then timers are generated at the software level and are less accurate than they would have been with hardware timestamps.



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.

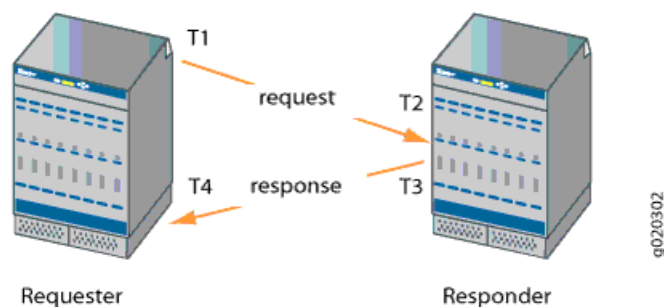
You should configure both the requester and the responder (see Figure 1 on page 2) to timestamp the RPM packets in order to get more meaningful results. If you do not configure timestamps on the responder, for example, if the responder does not support hardware timestamps, RPM can only report round-trip measurements that include the processing time on the responder.



NOTE: Hardware timestamps are supported on all EX-series switches and on the Adaptive Services and MultiServices PICs for M-series and T-series routing platforms.

Figure 1 on page 2 shows the timestamps:

Figure 1: RPM Timestamps



- T1 is the time the packet leaves the requester port.
- T2 is the time the responder receives the packet.
- T3 is the time the responder sends the response.
- T4 is the time the requester receives the response.

The round-trip time is $(T2 - T1) + (T4 - T3)$. If the responder does not support hardware timestamps, then the round-trip time is $(T4 - T1) / 2$, and thus includes the processing time of the responder.

You can use RPM probes to find the following time measurements:

- Minimum round-trip time
- Maximum round-trip time
- Average round-trip time
- Standard deviation of the round-trip time
- Jitter of the round-trip time—Difference between the minimum and maximum round-trip time



NOTE: Configure timestamps by specifying the destination interface using the `destination-interface` statement at the `[edit services rpm probe probe-owner test test-name]` hierarchy level on the requester. (For configuration details, see the *JUNOS Software Services Interfaces Configuration Guide* at <http://www.juniper.net/techpubs/software/junos/junos93>.) Also, on the responder, specify the RPM client (the requester) using the `rpm client` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level.

The RPM feature provides an additional configuration option to set one-way hardware timestamps. Use one-way timestamps when you want information about one-way time, rather than round-trip times, for packets to traverse the network between the requester and the responder. As shown in Figure 1 on page 2, one-way timestamps represent the time $T2 - T1$ and the time from $T4 - T3$. Use one-way timestamps when you want to gather information about delay in each direction and to find egress and ingress jitter values.



NOTE: For correct one-way measurement, the clocks of the requester and responder must be synchronized. If the clocks are not synchronized, one-way jitter measurements and calculations can include significant variations, in some cases orders of magnitude greater than the round-trip times.

When you enable one-way timestamps in a probe, the following one-way measurements are reported:

- Minimum, maximum, standard deviation, and jitter measurements for egress and ingress times
- Number of probes sent

- Number of probe responses received
- Percentage of lost probes

Limitations of RPM

- Two-way Active Measurement Protocol (TWAMP) is not supported on EX-series switches.
- EX-series switches do not support user-configured class-of-service (CoS) classifiers or prioritization of RPM packets over regular data packets received on an input interface.
- Timestamps:
 - If the responder does not support hardware timestamps, RPM can only report the round-trip measurements and cannot calculate round-trip jitter.
 - EX-series switches do not support hardware timestamps for HTTP and TCP probes.
 - Timestamps apply only to IPv4 traffic.

Related Topics

- *JUNOS Software Services Interfaces Configuration Guide* at <http://www.juniper.net/techpubs/software/junos/junos93>
- Understanding Using sFlow Technology for Network Monitoring on an EX-series Switch
- Configuring SNMP (J-Web Procedure)
- Monitoring Hosts Using the J-Web Ping Host Tool
- Monitoring Network Traffic Using Traceroute