CA Spectrum®

Service Performance Manager User Guide

Release 9.4

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

CA Technologies Product References

This document references the following CA Technologies products:

- CA Spectrum® Service Performance Manager (SPM)
- CA Spectrum® Report Manager (Report Manager)
- CA eHealth® Performance Manager (CA eHealth)
- CA SystemEDGE

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction 9

Chapter 2: Finding Components 21

Chapter 3: Working with Performance Tests 27

Chapter 5: Viewing Service Performance Manager Information 65

Chapter 6: Generating Reports on Test Data 73

Chapter 7: Using the Command Line Interface (CLI) to Manage Tests 79

Appendix A: Troubleshooting 113

Chapter 1: Introduction

This section contains the following topics:

Service Performance Manager Concepts

Service Performance Manager (SPM) lets you create, run, and manage performance tests that are supported by third-party products. The products from various vendors that CA Spectrum manages perform their own testing to address multiple network management requirements. The following goals are examples of the types of testing that are supported:

- Testing IT service delivery standards—You can simulate transactions, such as HTTP transactions, login validations, or file transfers to establish delivery benchmarks. You can then measure service delivery to consumers and develop realistic service-level agreements.
- Capacity planning— Run tests to determine whether service demands by consumers are underutilizing or exceeding current IT infrastructure capacity.
- Proactive fault management—You can pinpoint service delivery degradation trends before they impact service consumers.

The topics in this section describe the Service Performance Manager components that let you configure and run performance tests.

Test Hosts

A *test host* is a model of a device or software agent that supports one or more performance tests for IT services. CA Spectrum creates a test host model of type RTM_TestHost during model discovery for each device that Service Performance Manager supports.

Some examples of test host devices and agents are a Cisco router, a Sun Workstation running iAgent, and a SpectroSERVER.

Important! Supported devices and agents must be modeled with read/write community strings to run Service Performance Manager tests. Attempts to run tests on test hosts (except for SpectroSERVERs) that are not modeled with a read/write community string cause an alarm on the test host model.

Configure the Application Model

You can configure the community string of the application model that Service Performance Manager uses. For example, you want to create the device model with a read-only community string. In such a case, you can configure the community string of the Service Performance Manager application model.

Note: Performance Agents and MIBs list tests that are supported by the performance agents and the associated CA Spectrum application model type. For more information, see Performance Agents and MIBs (see page 13).

Follow these steps:

1. Click the Locater tab.
2. Expand the Application Models folder.
3. Double-click the By Device IP Address field, and enter the device IP address.
4. Filter and select the appropriate application model.

   For example, for Cisco IP SLA supporting hosts, enter CiscoRTTMonApp.
5. Click the Attributes tab.
6. Filter for the Community_Name.
7. Select Community_Name/0x10024 and select the right arrow.

   The attribute appears in the right panel.
8. Double-click to select and change the value.

   The community string of the application model is now configured.

Tests

A performance or response-time test is an IT service operation that returns a result. Retrieving a web page, downloading a file, and establishing a TCP connection are all examples of common service operations. A single test returns a result that can help you troubleshoot a performance issue. A group of tests return aggregate results that can help you evaluate service viability over a particular timeframe. You can also derive baseline standards that you can factor into infrastructure decision-making.

Service Performance Manager lets you create tests (model type RTM_Test) for your test hosts and discover tests that are configured on managed devices. You can schedule tests and also run them on demand. You can specify test thresholds and can incorporate tests into service management and service-level agreements.

Supported performance tests fall into the following three categories:

- Network response-time tests: Basic network response-time tests.
- Network service response-time tests: Measure the response times of essential network services.
- Network application response-time tests: Measure the response times of essential network applications.

Network Response Time Tests

Network response time tests are the most basic type of network response time tests. The following network response time tests are supported:

ICMP Ping

Tests the ICMP Echo Request messages from the test host to the destination address. If the test host and the source addresses are not same, then another ICMP Echo Request is issued from the test host to the source address. The resulting ICMP Echo Reply messages are used to determine the round-trip time between the source address and the destination address. A second metric, packet loss, is included in the results. When a series of ICMP Echo requests are made, which is typical of these tests, a coarse measure of packet loss is possible.

Jitter

Tests latency and losses between two endpoints. This test is designed to measure the quality of the network for applications that cannot tolerate loss or latency (such as VoIP).

Traceroute

Tests round-trip ICMP Echo from the host address to each layer with three hops in the discovered path.

Network Service Response Time Tests

Network service response time tests measure the response time of essential network services. The following network service response time tests are supported:

DHCP

Identifies the Dynamic Host Configuration Protocol IP address assignment.

DNS (Domain Name Service)

Translates the domain name to IP address.

Network Application Response Time Tests

Network application response time tests measure the response time of essential network applications. The following network application response time tests are supported:

Custom

Custom script execution.

FTP

Indicates the File Transfer Protocol transaction time.

HTTP/HTTPS

Indicates the Hyper Text Transfer Protocol transaction time.

POP3

Indicates the Post Office Protocol transaction time.

SMTP

Indicates the Simple Mail Transfer Protocol transaction time.

SQL Query

Indicates the SQL query response time.

TCP

Indicates the Transmission Control Protocol connection time.

UDP Echo

Indicates the User Datagram Protocol transmissions echo round-trip delay.

Test Templates

Test templates contain the parameters for a particular type of test. You can selectively apply templates to multiple test host models. Or you can automatically apply templates to test host models that are added to the Global Collection models. CA Spectrum monitors Global Collection content and automatically creates the test that the template specifies on test hosts that are added to the Global Collection. Regardless of how a test template is applied to test hosts, the result is the same: the test that the template defines is created on the test hosts.

More information:

Working with Test Templates (see page 57)

Alarms

Service Performance Manager generates various events representing significant occurrences that are related to response time testing. Some of these events produce alarms that notify you when a user-actionable event has occurred. For more information, see Event Codes (see page 119).

You can also configure Service Performance Manager to generate an alarm whenever the duration of a response time test exceeds a predetermined threshold. Such alarms can be isolated to a specific link or path. For more information, see Specify Alarm Thresholds for a Test (see page 50) and Alarms and Events (see page 70).

Performance Agents and MIBs

The following table lists performance agents and MIBs that are supported by Service Performance Manager. The tests that are supported for each agent or MIB are also given.

Agent/MIB	CA Spectrum Application Model Type	Tests
RFC2925	RFC2925App	ICMP Ping, Traceroute **Note:** You must verify with the vendor whether a particular device supports the RFC2925 MIB.
Cisco IOS IP SLAs Agent (Cisco IOS IP SLAs Agent is supported on Cisco routers running IOS 12.0 or greater.) **Note:** For full-mesh measurements between hubs, Cisco recommends using shadow routers that are dedicated for IOS IP SLAs. For more information, see the Cisco IOS IP SLAs documentation.	CiscoRTTMonApp	DHCP, DNS, FTP, HTTP, ICMP Ping, Jitter, TCP, UDP, ICMP_JITTER You can discover tests configured on Cisco agents with the SPM Test Discovery feature. For more information, see Discover Tests in the Network (see page 34).

Agent/MIB	CA Spectrum Application Model Type	Tests
CA eHealth SystemEDGE Service Availability agent	Emp_SvRsp_App	Custom, DNS, FTP, HTTP, HTTPS, ICMP Ping, POP3, SMTP, SQL Query, TCP You can discover tests configured on SystemEDGE agents with the SPM Test Discovery feature. Tests for SystemEDGE agents are discovered in read-only mode only. For more information, see Discover Tests in the Network (see page 34). **Note:** SystemEdge agents require the eHealth Service Availability module to run performance tests.
Network Harmoni SLAplus Agent OEM Vendors: Agilent Technologies, InfoVista, Peregrine Systems, Ericsson, Opticom, RedPoint, HP, Micromuse, Response Networks	HrmniSvcRspApp	DNS, HTTP, ICMP Ping
iAgent	SRISvcMonApp	DNS, FTP, HTTP, ICMP Ping, POP3
JUNOS Real Time Performance Monitor	JnprRFC2925ExtApp	ICMP Ping, Jitter, Traceroute
Other Support		
Cisco Ping MIB	CiscoPingApp	ICMP Ping
Wellfleet Ping MIB	WFPingApp	ICMP Ping

Note: It is only the current Cisco routers that support the RTTMON MIB. Older, pre-11.2 deployments support only the Cisco Ping MIB. Service Performance Manager does not support the Nortel Contivity Ping MIB (CONTIVITY-INFO-V1-MIB).

Service Performance Manager Features

Service Performance Manager supports multiple vendor and agent performance tests solutions and multiple implementation features.

Multiple Ways to Create Tests

You have the following options for creating tests with Service Performance Manager:

- Create a test from scratch.
- Create a version from a copy of another test.
- Use SPM Discovery to locate tests that are configured on test hosts.
- Apply test templates to Global Collection containers. When a test host is added to the container, a test with the settings in the template is created on the test host.

Test Scheduling

SPM offers scheduling capabilities to automate your performance testing. You can use preconfigured schedules that are provided by OneClick or you can create your own custom schedules. Scheduling tests lets you implement performance testing during peak and off-peak hours. You can then compare the results from each period and determine realistic performance standards.

For example, you want to schedule a test to run at a specific interval continually, such as 24 hours a day, 7 days a week. Or you can schedule tests to run during or after intervals when the infrastructure is in high demand. In either case, you can create test schedules that meet your requirements.

Automated Test Creation with Test Templates

Test templates let you create test configurations and apply them to multiple test hosts. Test templates leverage Global Collection container capabilities. By applying a template to a Global Collection container, you can automate the test creation process. The test that the template specifies is created for any test host that you add to the container that supports the test. Modifications to test parameters are also simple to perform. When you change template parameters, those changes extend to the parameters for all tests that are created from the template.

Single-Point Test Management

Service Performance Manager provides complete access and control over your test components on multiple landscapes from a single landscape. You can create, configure, locate, and manage tests from a single OneClick Console.

Report Options

You can generate summary and detailed performance test results in various text and graphical formats using Spectrum Report Manager. You can also use result data in the CA Spectrum SSLogger format by exporting it to text files.

Service Performance Manager Tests and Service Level Agreement Management

Performance testing is indispensable for establishing IT service-obligation benchmarks and monitoring service performance. SPM response time test results provide a more accurate measure of service performance and viability than a notification that reports whether a service is up or down. Service consumers often consider service delivery speed the determining factor in whether a service meets their requirements.

For example, a service consumer considers a 20-second wait for a web page to load because it takes 5 seconds on average to retrieve and load a page. Such a consumer can assume that the sluggish web service is unavailable, even though it is accessible.

Service Performance Manager lets you specify response time thresholds to measure service performance in terms of latency. These thresholds support service-level agreements that ensure a specified response time and meet the requirements of the consumer. You can create and manage services and service-level agreements in CA Spectrum. For more information, see the *Service Manager User Guide*.

User Roles

User access to SPM functionality depends on the rights that are granted to the user account. A CA Spectrum administrator can configure user roles and rights in OneClick. For more information, see the *Administrator Guide*.

Service Performance Manager for Operators

When you are logged in to Service Performance Manager as an operator, you can view information for tests and test hosts and can run existing response time tests. As an operator, you cannot create, delete, edit, or copy any tests. Operators cannot change the state of a test on any test hosts.

Service Performance Manager for Administrators

When you are logged in to Service Performance Manager as an administrator, you have full access to all functionality, including creating, editing, deleting, and discovering tests.

Getting Started

This section describes the procedure to access Service Performance Manager components and the basic tasks that you can perform from the OneClick Console. This section provides information about configuring security for tests and test hosts.

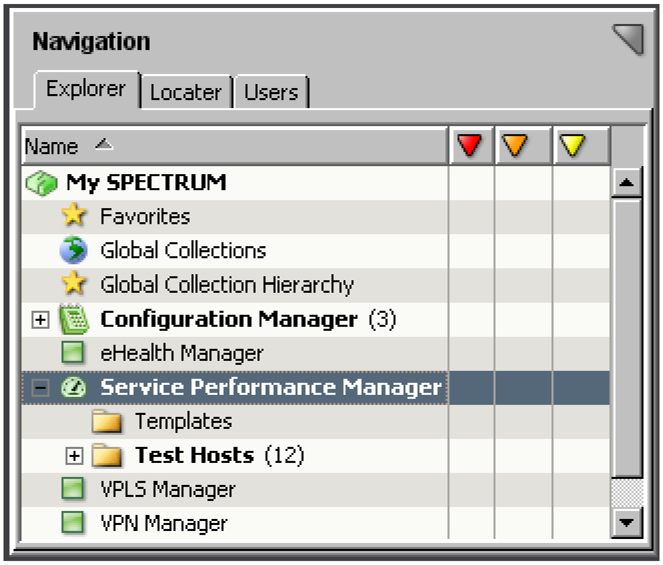
Access Service Performance Manager

You can access Service Performance Manager from the OneClick Console.

Follow these steps:

1. From the Explorer tab, select Service Performance Manager.

   The following image shows the navigation to access Service Performance Manager.



2. To display views, expand the Service Performance Manager node.

   The Templates and Test Hosts views appear.

Basic Tasks Overview

Once you have accessed Service Performance Manager in the OneClick Console Locater, perform the following basic tasks to work with its components:

- Locate a specific test component or group of components (tests, test hosts, test templates). For more information, see Finding Components (see page 21).
- Create and edit tests, configure test parameters, schedule tests, specify test thresholds, manually run tests, and discover tests on test hosts. For more information, see Working with Performance Tests (see page 27).

- Create and manage test templates and apply them to test hosts or to Global Collection containers that include test hosts. For more information, see Working with Test Templates (see page 57).
- Create, run, and edit tests from the Command Line Interface. For more information, see Creating and Managing RTM Tests with the Command Line Interface (CLI) (see page 79).
- Generate reports on tests with Spectrum Report Manager and use the available result data. For more information, see Generating Reports on Test Data (see page 73).

About Test Host and Test Security

A security string within the respective component controls security for test and test host models. You can use the security string to restrict access to test and test host models to authorized personnel only.

The security string originates from the device model. The test host model inherits the security string from the relevant device model. The test model later inherits the security string from the test host model.

Consider the following points when using test templates:

- When using test templates to create tests, the security string that is specified in the template is not propagated to the test model. The test model inherits its security string from the test host.
- When applying test templates to Global Containers, tests are created for the test hosts where you are authorized.

Note: You must have privileges to invoke detailed views of CA Spectrum models in OneClick Console and to modify security string settings for models. You can also set up CA Spectrum model security. For more information, see the *Administrator Guide*.

Verify the following procedures to set or modify a security string for a test host or test:

- Secure a Test Host (see page 19)
- Secure a Test (see page 19)
- Overwrite a Security String (see page 19)

Secure a Test Host

You can secure a test host by specifying a security string for it.

Follow these steps:

1. In the Contents panel on the Information tab, expand Test Host Details for the test host that you want to secure.
2. Click set for the Security String parameter, and specify the security string.

   Permission to access the test host is now granted only to privileged users defined by the security string entered.

   Note: All tests that are associated with a secured test host automatically inherit the host security string. You can override or remove a security string at a test level (or test host level). For more information, see Overwrite a Security String (see page 19).

Secure a Test

You can secure a test by specifying a security string for it.

Follow these steps:

1. In the Component Detail panel on the Information tab, expand Test Details, General for the test to secure.
2. Click set for the Security String parameter.
3. Specify the security string.

   Permission to access the test is now granted only to the privileged users defined by the security string.

Override a Security String

You can override security strings for test hosts or tests (if necessary).

Follow these steps:

1. Access the Security String parameter for the component whose security string you want to override. For more information, see Secure a Test Host (see page 19) or Secure a Test (see page 19).
2. Click set for the Security String parameter.
3. Edit or remove the security string.

   The security string is modified.

Chapter 2: Finding Components

Service Performance Manager provides multiple options to find existing tests, test hosts, and test templates in CA Spectrum. For more information about search features, see the *Administrator Guide*.

All Test Component Searches

This search category lets you search for all test hosts, tests, and test templates that are modeled in CA Spectrum. Using generated search results, you can select an item, view information about it, and can perform any operation that it supports.

Follow these steps:

1. Expand Service Performance Manager in the Explorer tab.

   The Templates and Test Hosts folders appear.

2. Expand the Templates folder.

   A list of all templates in the DSS environment is displayed.

   Note: If you select the Templates folder, the list of templates also appears in the List tab of the Contents panel.

3. To display all test hosts, expand a test host.

   All test models under that host are displayed.

   Note: If you select the Test Hosts folder, the list of test hosts also appears in the List tab of the Contents panel.

4. To display all tests, expand SPM folder in the Locater tab.
5. Double-click the All Tests option to launch the search.
6. Specify appropriate landscape information in the "Select Landscapes to Search" dialog and click OK.

   Search results appear in the Results tab of the Contents panel.

Criteria-Based Test Host Searches

You can search for test hosts that are modeled in CA Spectrum that meet the criteria you specify. This section describes the procedure to perform criteria-based test host searches and the supported criteria for test host searches.

How to Perform Criteria-Based Test Host Searches

You can perform a criteria-based search for test hosts.

Follow these steps:

1. Click the Locater tab in the Navigation panel.
2. Expand the SPM folder.
3. Expand the Tests Hosts By folder.
4. Select the type of criteria-based test host search to run.
5. Click the Search button.

   Note: Depending on the search that you select, you can enter values (typically IP addresses) in a Search dialog before the search is executed.

   Search results appear in the Results tab in the OneClick Contents panel. You can select an item that a search returned, view information about it, and can perform any operation that it supports.

Supported Criteria for Test Host Searches

You can perform a criteria-based test host searches based on the supported criteria for test host searches. Verify the following supported criteria for test host searches:

IP Address

Finds the test host with the Network Address or tests hosts that are associated with the address you specify in the Search dialog.

Note: The Search dialog does not support searching on partial IPs (for example, 10.253).

State

Finds test hosts in the following states:

Active

Test hosts that have been activated.

Contact Lost

Test hosts that have stopped responding to polls.

Inactive

Test hosts that have not been activated or have been deactivated.

Maintenance

Test hosts that are in maintenance mode.

Test Discovery Support

Supported

Finds test hosts that support test discovery.

Unsupported

Finds the test host that does not support test discovery.

Test Type Support

Finds test hosts that support a particular test type.

Criteria-Based Test Searches

You can search for tests that are modeled in CA Spectrum and that meet criteria you specify by using the Tests By option. This section describes the procedure to perform criteria-based search for a test and the supported criteria for test searches.

Perform Criteria-Based Test Searches

You can perform a criteria-based search for a test.

Follow these steps:

1. Click the Locater tab in the Navigation panel.
2. Expand the SPM folder.
3. Expand the Tests By folder.
4. Select the type of criteria-based test search to run.
5. Click the Search button.

   Note: Depending on the search that you select, you are prompted for additional values (such as IP addresses) before the search is executed.

   Search results appear in the Results tab in the OneClick Contents panel. You can select an item that a search returned, view information about it, and can perform any operation that it supports.

Supported Criteria for Test Searches

You can perform a criteria-based test search. Verify the following supported criteria for test searches:

Configuration Parameters

Find tests that meet the following criteria as specified in the Search dialog:

- Destination Address
- Destination Address and Port Number
- Source Address
- Source Address and Destination Address
- Source Address, Destination Address, and Port Number

You can enter partial address strings (for example, 138.42) for the Source Address and Destination addresses. Searches with the destination port set to 0 return tests for which destination port is not applicable.

Discovery State

Find tests that meet the following criteria that are related to SPM Discovery:

Discovery Read-Only

Tests that are discovered in Read-Only mode through SPM Discovery.

Discovery Read/Write

Tests that are discovered in Read/Write mode through SPM Discovery.

Other

Tests that were created by VPN Manager, other IP service applications, or the Command Line Interface.

RTM Domain

Tests that were created using the user interface (and not through SPM Discovery).

Stale Different Type

Tests that were discovered by Service Performance Manager with a corresponding test on the device of a different test type.

Stale Entry Not Present

Tests that were discovered by Service Performance Manager that no longer have a corresponding test on the device. For more information, see Discover Tests in the Network (see page 34).

Name

Find a test that is based on the Test Name you specify in the Search dialog.

Scheduled

Find all scheduled tests.

Status

Find a test using one of the following test status options:

- Bad Community String
- Bad Configuration
- Device Disabled
- Ready To Run
- Running
- Scheduled
- Stopped
- Timeout
- User Disabled

Threshold Exceeded

See a list of all of the tests exceeding their thresholds.

Type

Find all tests of a particular type.

Chapter 3: Working with Performance Tests

This section describes what tests are available and how to create them in your environment. Using CA Spectrum Command Line Interface, you can create and manage response time tests. For more information, see Creating and Managing RTM Tests with Command Line Interface (CLI) (see page 79).

This section contains the following topics:

Supported Test Types

This section includes information about specific test types that you can review before you create or can run the tests.

Custom Tests

Custom tests give you the flexibility to specify a custom script to run for the test. This test allows you to verify that the important services or other tasks are working efficiently.

Note: Custom tests are only for SystemEDGE hosts.

DHCP Tests

DHCP tests measure the round-trip time (latency) required to get an IP address. The DHCP server must be on the same subnet as the test host performing the DHCP test. To configure the test host to work with your DHCP server IP address, see the documentation for the device. For DHCP tests to work on a router, one of the neighboring routers must be a DHCP agent or relay. For more information, see the documentation for your device.

Note: DHCP test latency result values can exceed the timeout value for tests that are run on Cisco router test hosts. These values result from a known issue with Cisco IOS 12.2(2)T (see page 114).

DNS Tests

DNS tests measure DNS lookup time. DNS-based host name-to-address translation must be enabled on the test host device performing the DNS test. You can verify whether DNS lookup is enabled and can enable it. For more information, see the documentation for the device.

DNS test results include the following metrics:

- Latency
- Packet Loss

FTP Tests

FTP tests measure the round-trip time to transfer a file.

FTP test results include the following metrics:

- Latency
- Packet Loss

Note: FTP tests that are run on Cisco test hosts using the RTTMON MIB require the username, password, and filename. However, FTP tests that are run on SystemEDGE Service Availability test hosts require a username and password.

HTTP Tests

HTTP tests measure the round-trip time to get a web page.

HTTP test results include the following metrics:

- Latency
- HTTP DNS Resolution Time
- HTTP TCP Connection Time
- HTTP Download Time

Considerations

- HTTP tests that are performed from Harmoni and iAgent test hosts generate only latency results.
- An HTTP test can fail on some Cisco systems using HTTP 1.1. For more information, see Firmware Issues (see page 113).

- The HTTP version configuration setting is only available for HTTP tests that are run from Cisco test hosts. The Proxy URL setting is only available for HTTP tests that are run from Cisco and CA eHealth SystemEDGE Service Availability test hosts. For more information, see Configure Advanced Parameters (see page 45).
- Service Performance Manager HTTP tests that require authentication are not supported on Cisco test hosts.

HTTPS Tests

HTTPS tests measure the round-trip time to get a web page over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. An HTTPS test measures the same metrics as an HTTP test.

ICMP (Ping) Tests

ICMP (Ping) tests measure round-trip time from a source to a destination address.

ICMP test results include the following metrics:

- Latency
- Packet Loss

Note: Cisco and Juniper test hosts support Virtual Routing and Forwarding (VRF) Ping tests.

Considerations

- When using the Cisco IOS IP SLAs Agent, you can configure the ICMP Echo operation payload size by setting the request size. The router adds 36 bytes to the size specified. For example, if the request size is 28 bytes, the actual ICMP Packet size is 64 bytes (of IP packet). For more information, see the *Cisco IOS IP SLAs Agent Documentation*.
- The Harmoni agent does not support the configuration of sample count or packet size for ICMP Ping tests.

Jitter Tests

Jitter tests measure both latency and loss between a test host and a voice-enabled endpoint. However, they add a finer measure of the statistical behavior of a sequence of requests. The Mean Opinion Scoring (MOS) is also available from Cisco test hosts. The MOS provides a numerical measure of the quality of human speech at the receiver. Jitter test results include the following metrics, depending on the test host:

- Destination to Source Packet Loss
- Jitter Busies
- Jitter Egress
- Jitter Ingress
- Jitter Positive Destination to Source
- Jitter Positive Source to Destination
- Jitter Negative Destination to Source
- Jitter Negative Source to Destination
- Late Arrival Packet
- Latency
- Mean Opinion Score
- Missing in Action Packet
- Packet Loss
- Source to Destination Packet Loss

Jitter tests can be configured to target a destination port that is listening for Jitter traffic. For example, many Cisco devices running IOS IP SLAs use Port 16386. Failure to configure the port can result in test timeouts. Set the Destination Port parameter in the General options for Jitter tests. For more information, see Configure General Parameters (see page 40).

POP3 Tests

POP3 tests measure POP3 response (transaction) time.

POP3 test results include the following metrics:

- Latency
- Packet Loss

SMTP Tests

SMTP Tests measures SMTP mail server response (transaction) time.

SMTP test results include the following metrics:

- Latency
- Packet Loss

SQL Query Tests

SQL Query tests confirm that SQL database servers are available by processing short queries that you specify.

Note: SQL Query tests are for SystemEDGE hosts only.

TCP Tests

TCP tests measure the time that is required to create a TCP connection.

TCP Connection test results include the following metrics:

- Latency
- Packet Loss

Trace Route Tests

Trace route discovers the layer three hops between the source and destination addresses. These tests also return a round-trip ICMP Echo measurement from the host address to each hop in the path.

Trace route test results include the following metrics:

- Latency
- Packet Loss
- For each hop, IP address and round-trip time

Note: Cisco and Juniper test hosts support Virtual Routing and Forwarding (VRF) trace route tests.

UDP Echo Tests

UDP Echo measures round-trip delay.

UDP Echo tests return Latency and Packet Loss results.

UDP tests must be configured to target a destination port that is listening for UDP traffic. For example, many Cisco devices running IOS IP SLAs use port 1967 and UNIX systems use port 7. Failure to configure the port can result in timeouts for UDP tests. Set the Destination Port parameter in the General options for UDP tests. For more information, see Configure General Parameters (see page 40).

ICMP_JITTER

ICMP_JITTER tests measure end-to-end performance metrics like latency, round-trip time, jitter (inter-packet delay variance), and packet loss between a Cisco device (source) and any other IP device (destination).

ICMP_JITTER test results include the following metrics, depending on the test host:

- Latency
- Packet Loss
- Late Arrival Packet
- Jitter Busies
- Jitter Positive Source to Destination
- Jitter Positive Destination to Source
- Jitter Negative Source to Destination
- Jitter Negative Destination to Source
- Packet out of Sequence SD (Source to Destination)
- Packet out of Sequence DS (Destination to Source)
- Packet out of Sequence BOTH (SD and DS)
- Packet Skipped

Create Tests

You can create a performance test from scratch, or you can use an existing test as a starting point.

You can create tests on hosts that have not been activated. But you must activate test hosts before running the tests. For more information, see Activate and Deactivate Test Hosts (see page 53).

You can also discover preconfigured tests on test hosts using SPM Discovery. Discovery models tests that have been created on test hosts using a method other than Service Performance Manager, such as the command line. For more information, see Discover Tests in the Network (see page 34).

Create a Test

You can create a test of any type that the test host supports.

Follow these steps:

1. Expand Service Performance Manager in the Explorer tab.

   The Templates and Test Hosts folders appear.

2. Expand the Test Hosts folder.

   A list of all test hosts in the DSS environment is displayed.

   Note: Expand a test host to see all test models that exist for that host.

3. Right-click the test host for which you want to create the test.
4. Select New Test and then select a test type.

   The New Test dialog opens. This dialog lets you configure test parameters.

5. Configure test settings and click OK.

   The new test is saved. Information about the new test appears on the Information tab in the Component Detail panel for the test host in the Test List table.

Create a Different Version of an Existing Test

You can create a test by saving a unique version of an existing test. The test can include the same settings, but a different name. You can save the new test to the base test host or to a different test host.

Note: You cannot copy tests between domains that are running different versions of CA Spectrum.

Follow these steps:

1. Expand Service Performance Manager in the Explorer tab.

   The Templates and Test Hosts folders appear.

2. Expand the Test Hosts folder.

   A list of all test hosts in the DSS environment is displayed. You can see a plus sign (+) for test hosts with existing test models.

3. Expand the test host whose test model you want to copy.

   A list of tests that are defined for that test is displayed.

4. Right-click the test, and select Copy Test.

   The Copy Test dialog opens, which lets you configure test parameters for the new test.

   Note: Copied tests are disabled by default, and "_COPY" is appended to the test name.

5. (Optional) Rename the test.

6. Modify test settings, and click OK.

   The new test is saved. Information about the test appears on the Information tab in the Component Detail panel for the test host in the Test List table.

Discover Tests in the Network

SPM Test Discovery lets you discover and model performance tests that are configured on test hosts but not configured with Service Performance Manager.

Considerations

- Administrator role privileges are required to use SPM Test Discovery.
- Use a device that SPM Test Discovery supports.

When you run a test Discovery, you are prompted to select the Discovery mode. The following two Discovery modes determine how the tests are created in Service Performance Manager:

- Read-Only Discovery Mode (see page 34)
- Read/Write Discovery Mode (see page 35)

Read-Only Discovery Mode

When you discover tests in read-only mode, you cannot edit test configurations after the tests are modeled in CA Spectrum. Because, you do not have SNMP *set* privileges to tests. Test Discovery takes schedule information from the tests that are configured on the device and reads test results at the appropriate interval.

Considerations

- Administrator access to read-only tests is similar to that of the Operator role, but it includes full access to Threshold parameters. For more information, see Specify Alarm Thresholds for a Test (see page 50).
- Read-only tests cannot be run manually; they must be scheduled.
- Sample Count is always 1.
- You can copy read-only tests to create tests that can be modified in Service Performance Manager.
- You can verify that data from read-only tests is available for response time reports, which you can generate with Spectrum Report Manager. Confirm that the test is in the Active state at the time of the read-only Discovery. You can also verify that the Events service indication in OneClick shows the Up status.

Read/Write Discovery Mode

When you discover tests in read/write mode, you can edit test configurations after the tests are modeled in CA Spectrum. SNMP *set* privileges to the tests are required. You can handle tests on these test hosts exactly like tests that are created manually in Service Performance Manager. Therefore, you can run tests on demand and can stop and edit. For more information, see Configure Tests (see page 39).

Considerations

- If the test is activated on the device, the Schedule State field for the Schedule parameter field is set to Enabled.
- Sample Count is set to 1.

Set the Test Name for Cisco IP SLA Tests

When discovering Cisco IP SLA tests in CA Spectrum for Cisco routers, the Tag value of the Cisco IP SLA test can be used as the test name in Service Performance Manager. Select a setting to enable this feature.

Note: This option is available for Cisco routers and for tests that were discovered using SPM Test Discovery only.

Follow these steps:

1. Select Service Performance Manager in the Explorer tab.

   Information about Service Performance Manager appears in the Information tab of the Contents panel.

2. Expand the General Information subview.

3. Modify the following field:

   Use Tag Field as Test Name for Cisco Test Host Discovery

   Specifies whether the Tag value is used as the test name during SPM Test Discovery.

   Note: For tests created in CA Spectrum, this setting has no effect.

Run Discovery

You can run test Discovery on a single test host.

Follow these steps:

1. In the Explorer tab in the Navigation panel, under Test Hosts, right-click the test host where you want to run Discovery.

2. Select Discover Tests from the right-click menu.

   If the selected test host supports both Read-Only and Read/Write Discovery modes, the Discover Tests: Select Discovery Mode dialog opens.

   The Discover Tests option is not available in the menu if the host does not support Discovery.

3. Select the appropriate option for the test discovery mode you want to run: Read-Only or Read/Write.

   Wwhen Discovery completes, the Discover Tests Complete dialog indicates how many tests were created or updated.

You can also locate multiple test hosts that support test discovery and run test discovery on multiple hosts.

Follow these steps:

1. In the Locater tab in the Navigation panel, expand the SPM folder.

2. Run the Test Hosts By, Test Discovery Support, Supported search to locate Discovery-compatible test hosts.

   The Contents panel lists test hosts that support test Discovery.

3. Select one or more test hosts where you want to discover tests, and click the Discover Tests icon.

   Note: The Discover Tests icon is disabled if a selected test host is not active, or if contact with the host is not established. For more information, see Activate and Deactivate Test Hosts (see page 53).

   If the selected test host supports both Read-Only and Read/Write discovery modes, the Discover Tests: Select Discovery Mode dialog opens.

4. Select the appropriate option for the test Discovery mode you want to run: Read-Only or Read/Write.

   When Discovery completes, the Discover Tests Complete dialog indicates how many tests were created or updated.

SPM Test Discovery Event Codes

The Events tab in the Component Detail panel provides results from the Discovery on the test host. The following list summarizes SPM Test Discovery event codes and descriptions:

SPM Test No Longer On Device Event (0x04560059)

Occurs when SPM Test Discovery fails to match an existing SPM Read-Only test to a table entry on the device, this event and a corresponding yellow alarm is generated on the test model.

SPM Test No Longer Running On Device Event (0x0456005a)

Occurs when SPM reads the test results and detects that the numberOfPktsSent object on the device has not increased. The operational state on the device is also read and found to be InActive. This event is generated, and the following actions occur:

- No data is processed.
- Schedule state on the SPM test is set to Disabled, and no more data is read.

SPM Duplicate Result Event (0x0456005b)

Occurs when SPM reads the test results and detects that the numberOfPktsSent object on the device has not increased. The operational state on the device is also read and found to be Active. This event is generated, and the following actions occur:

- No data is processed.
- Schedule state on the SPM test remains Enabled; therefore data is processed from the next scheduled test.

SPM Test Discovery Completion Event (0x0456005c)

Generated after an SPM Test Discovery has run. Indicates the mode (Read-Only or Read/Write) in which the Discovery was run. Can contain any of the following error output:

- No Errors
- No SPM Tests Were Discovered
- Test type is invalid
- Test name is null
- Test timeout is 0
- Test frequency is 0
- Test packet size is 0
- Test sample count is 0
- Test port number is invalid
- Test IP Address is invalid
- Test URL is invalid
- Test host name is invalid
- Test user name is invalid
- Test password is invalid
- Test filename is invalid

SPM Test Type Mismatch Event (0x0456005d)

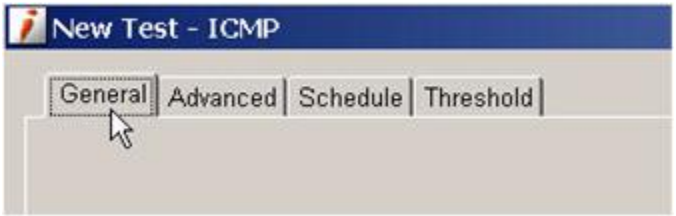
Occurs when SPM Test Discovery matches an SPM Read-Only test to a table entry on the device that is of the wrong test type. Generates this event and a corresponding yellow alarm on the test model.

SPM Stale Test Clear Event (0x0456005e)

Clears 0x4560059 or 0x456005d if subsequent SPM Test Discovery clears the condition.

Configure Tests

Whenever you issue a create, copy, or edit test command, Service Performance Manager displays a test configuration dialog. You can specify test parameters, set up a test schedule, and specify test thresholds. The following image shows example test configuration categories:



The configuration options depend on the type of test. Some of the options that are discussed in the following procedure do not apply to all types of test.

Follow these steps:

1. Enter values for the test in the parameter categories for your particular test.

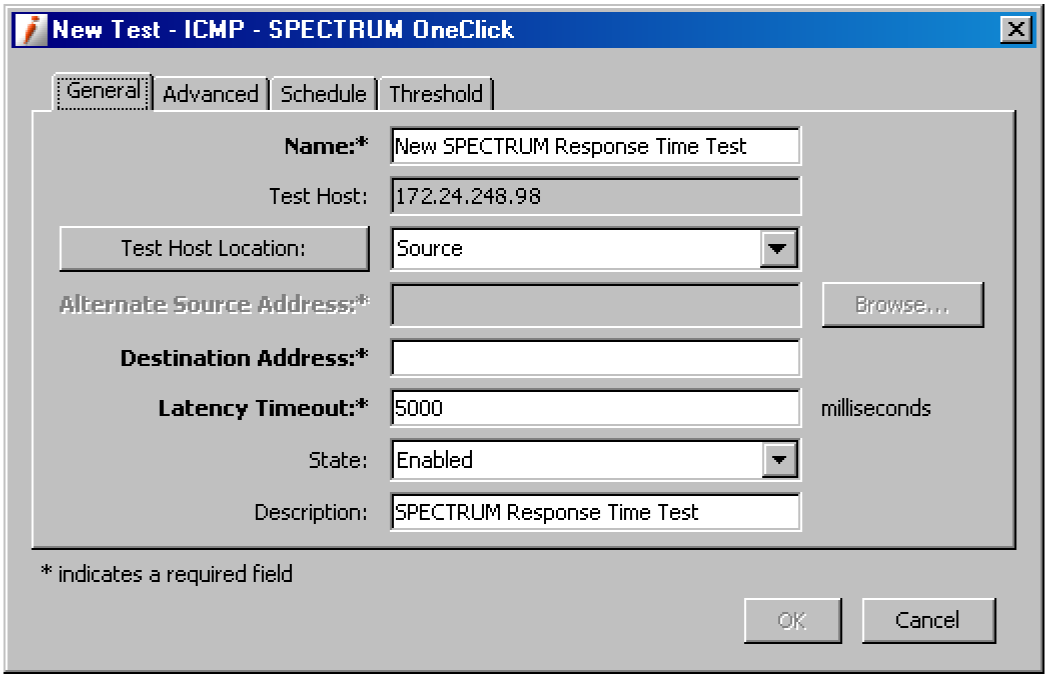
   For example, test scheduling is disabled by default. If you are not interested in scheduling test runs, ignore the scheduling parameters. The same applies to the test thresholds.

2. Click OK in each parameter category to save your settings.

   Note: The OK button is disabled if you do not enter required values.

Configure General Parameters

The General tab lets you configure required parameters for a test. The following image shows an example configuration dialog for an ICMP (Ping) test.



Name:* New SPECTRUM Response Time Test

Test Host: 172.24.248.98

Test Host Location: Source

Alternate Source Address:*

Destination Address:*

Latency Timeout:* 5000 milliseconds

State: Enabled

Description: SPECTRUM Response Time Test

* indicates a required field

Standard General Parameters

The following general parameters are available for all performance tests that Service Performance Manager supports:

Name

Specifies the test name.

Default: New SPECTRUM Response Time Test

Test Host

Indicates the IP address of the test host for the test.

Latency Timeout

Specifies the number of milliseconds for the response. If no response is received before this timeout occurs, CA Spectrum generates a timeout event. Any response that arrives after this timeout is ignored. Set the timeout higher than the threshold setting.

Default: 5000 milliseconds

Note: The Harmoni agent does not support latency timeout configuration.

State

Enables and disables the test.

Default: Enabled

Description

Specifies test annotations.

Default: SPECTRUM Response Time Test

General Parameters for Specific Test Types

The following parameters may be included under the General tab, depending on the type of test:

Alternate Source Address

Specifies the IPv4 address or hostname of the test source location when it is not the test host. For example, specifies a mid-path location and extended path location for ICMP Ping test scenarios.

Note: IPv6 addresses are not supported.

Browse

Lets you select an Alternate Source Address if the test host where you are configuring the test is not the source (ICMP). Or select another test host if you are copying test configurations.

Codec Type

Specifies the VOIP codec (audio compression/decompression) type to test: G.711 U-law, G.711 A-law and G.729A.

Note: You can set a voice quality threshold value (100 - 500) for the selected codec with the Mean Opinion Score parameter under the Threshold tab.

Connect String

Provides the string of commands that are used to connect to the database. For example,

```
jdbc:mysql://172.22.246.43/mysql?user=root&password=root
```

Database Name

Specifies the name of the database.

Database Type

Specifies the type of database to test. Correct drivers must be installed on the SystemEDGE server.

Destination Address

Specifies the destination address for the test except those of type DHCP, DNS, HTTP. You can enter an IPv4 address or a host name.

Note: IPv6 addresses are not supported.

Destination DNS Server

Specifies the destination address of the DNS server for DNS tests. You can enter an IP address or a host name.

Destination Port

Specifies the port number where the service is running. For Mean Opinion Score (MOS) support in Jitter tests, the destination port can be an even-numbered port in the range 16384 through 32766 or 49152 through 65534.

Destination URL

Specifies the URL used in HTTP and HTTPS tests.

File Name

Specifies the file path that is used for the FTP test.

Lookup Name

Specifies the IP address, host name, or fully qualified domain name (FQDN) of the host in DNS tests.

Note: Some agents, such as iAgent, require the use of an FQDN rather than a host name.

Operation Type

Specifies the type of FTP operation to test.

Login

This test logs in using the specified user name and password and then logs out.

Get

This test logs in and reads the remote file that is specified in the File Name field (but does not perform a write operation), then logs out.

Put

This test logs in and writes the local file that is specified in the File Name field out to the FTP server, then logs out. If the remote directory does not have write permissions, the test fails.

Default: Login

Note: Operation Type is available for FTP tests for SystemEDGE hosts only.

Password

Specifies the password for FTP, HTTP, HTTPS, or POP3 test authentication. For SQL Query, this password is used for database access.

Query String

Specifies the query statement to execute.

Script Path

Specifies the name and location of a valid script.

SQL Database Server

Indicates the host name or IP address of the SQL database server.

SQL Driver

Specifies the name of the SQL driver. For example, `com.mysql.jdbc.Driver`

Test Host Location

Specifies the location of the test host on the path between the source and destination for ICMP Ping tests.

Default: Source

Note: See About the Test Host Location Parameter (see page 43) for more information.

User Name

Specifies the user name for FTP, HTTP, HTTPS, or POP3 test authentication. For SMTP, you can use this email address to test. For SQL Query, this is the user name for database access.

Voice Test

Specifies whether to test voice quality for Jitter tests.

About the Test Host Location Parameter

Test host location refers to the path between the source and destination of a response time test. The location is critical to response time measurement.

Test host locations:

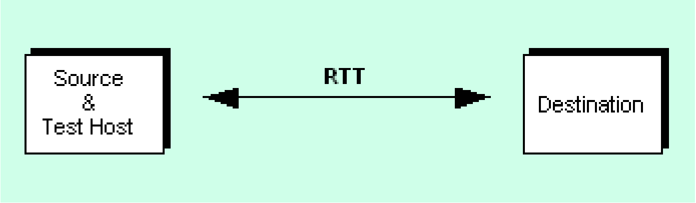
- **Source:** the test host is the source of the test.
- **Mid path:** the test host is located between the source and destination points.
- **Extended path:** test host is not located between the source and destination points.

Note: Only ICMP Ping tests support mid path or extended path tests.

Mid path and Extended path tests are useful only when the source or destination address is not a test host. In both of these test types, you can configure test host location.

Source Location

In the most common response time test scenario, the source, or starting point, of the test is also a test host, as shown in the following diagram:



In this case, the test host generates a transaction directly with the destination and measures the RTT.

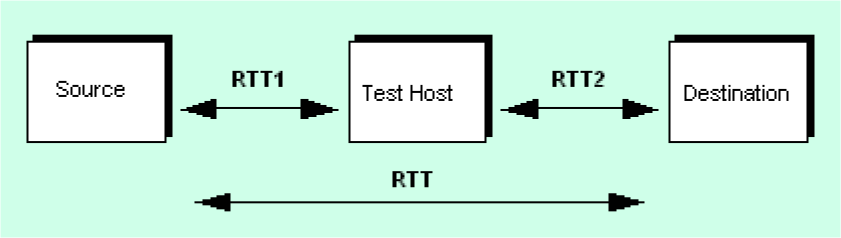
When the source of a test is a test host, response time measurements are the most direct and accurate. For this reason, you can set up tests with a test host as the source whenever possible.

Mid Path Location

In a mid path test configuration, a test host lies on the path between the source and destination points for which RTT is being measured. The source of the test is not capable of being a test host, so it cannot initiate or perform any response time measurements. Use the following calculation to measure the response time for a mid path test:

> Response time for a mid path test = (response time (RTT1) from test host to the source) + (response time (RTT2) from test host to the destination)

This value is a relative value which approximates actual RTT. The following image is an example of a mid path test configuration:

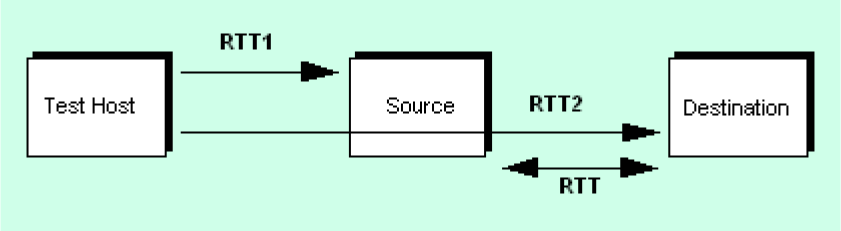


Extended Path Location

In an extended path test configuration, the source of the test is not capable of being a test host. In addition, no test host is located between the source and destination as in the Mid Path Location scenario. However, the source lies directly in the path between a test host and the destination. In this case, use the following calculation to measure the response time:

> Response time = (response time (RTT2) from the test host to the destination) — (response time (RTT1) from the test host to the source)

This value is a relative value which approximates actual RTT. The following image is an example of an extended path test configuration:



Configure Advanced Parameters

The Advanced tab lets you configure additional parameters for a given test type. Each test type has its own specific parameters.

Verify the following Advanced Parameters for all test types:

Alternate Packet Address

> Specifies an alternate source IP address instead of using the default network address of the device that is discovered in CA Spectrum.
>
> **Note:** The Alternate Packet Address field is available for all Cisco test hosts that support IOS IP SLAs Agent.

Alternate Packet Port

> Specifies an alternate packet port instead of using the default packet port of the device that is discovered in CA Spectrum.
>
> **Note:** The Alternate Packet Port field is available for all Cisco test hosts that support IOS IP SLAs Agent.

Delete Messages

> Specifies whether to delete the messages that were downloaded during the test or to leave the messages on the test system.
>
> **Default:** False
>
> **Note:** Delete Messages is available for POP3 tests for SystemEDGE hosts only.

Download Content

Specifies whether to download all images, frames, scripts, and applets with the core HTML code from the website or URL.

Default: False

Note: Download Content is available for HTTP and HTTPS tests for SystemEDGE hosts only.

Download Type

Specifies whether the first or all messages are downloaded for POP3 tests.

First

This option downloads only the first message for this user account.

All

This option downloads all messages for this user account.

Default: First

Note: Download Type is available for POP3 tests for SystemEDGE hosts only.

Fail On Content Error

Specifies whether any errors encountered while downloading images, frames, scripts, and applets cause the test to fail.

Default: False

Note: Fail On Content Error is available for HTTP and HTTPS tests for SystemEDGE hosts only.

Filter Timeout Data

Specifies whether the Performance tab the OneClick Component Detail panel displays all data or a subset of data minus timeouts.

Default: True

Frame Depth

The number of levels the test should traverse when downloading nested frames. The HTTP and HTTPS tests download all frames, images, external scripts, and applets during the page download. The measurement reflects the user experience when downloading a web page.

Default: 3

Note: Frame Depth is available for HTTP and HTTPS for SystemEDGE hosts only.

HTTP Version

Specifies the HTTP version (1.0 and 1.1) for HTTP tests.

Default: 1.1

Mail Body Size

Specifies the size (in bytes) of the test message to send.

Default: 1000

Note: Mail Body Size is available for SMTP tests for SystemEDGE hosts only.

Minimum Matches

The minimum number of times the search expression must be found. If the search expression is not found at least as many times as you specify in this field, the test fails.

Default: 1

Note: Minimum Matches are available for HTTP and HTTPS tests for SystemEDGE hosts only.

Outgoing User Name

Specifies the outgoing user name for SMTP authentication for SystemEDGE hosts.

Outgoing Password

Specifies the password for the outgoing user name for SMTP authentication for SystemEDGE hosts.

Packet Size

Specifies the value (in octets) that limits the size of the packets that are used in the test.

Note: The Harmoni agent does not support packet size configuration.

Proxy Password

Specifies the password for the Proxy User Name. The password is encrypted in the CA Spectrum database.

Note: Proxy Password is available for HTTP tests for Cisco routers and HTTP and HTTPS tests for SystemEDGE hosts only.

Proxy Server

Specifies the host name (the name or IP address) of the proxy server to use if the system from which you are testing does not have direct Internet access.

Note: Proxy Server is available for HTTP and HTTPS tests for SystemEDGE hosts only.

Proxy URL

Specifies the proxy URL for HTTP tests. For more information, see HTTP Tests (see page 28).

Proxy User Name

Specifies a valid user name to be authenticated on the specified proxy server.

Note: Proxy User Name is available for HTTP tests for Cisco routers and HTTP and HTTPS tests for SystemEDGE hosts only.

Sample Count

Specifies the number of times a test is performed during a test run.

Default: 5

Notes:

- For Cisco IP SLA tests, the agent supports a sample count of '1' only for all tests other than Jitter tests. For more information, see Considerations for CA eHealth and Cisco IP SLA Tests (see page 52).
- RTTMON may occasionally perform more than the specified sample count repetitions for a Service Performance Manager test.
- The Harmoni agent does not support the configuration of sample count.

Text Match

Specifies a regular expression or text string that you want to match on the pages you test.

Note: Text Match is available for HTTP and HTTPS tests for SystemEDGE hosts only.

Type of Service

Specifies the Type of Service (TOS) parameter for test packets that are sent by the test host. For example, create a response time test with the TOS parameter that VOIP uses and test the performance of the network in routing the packets.

The Type of Service octet in an IP datagram header enables packets with different TOS values to be routed differently.

Use SSL

Specifies whether to enable Secure Sockets Layer security in case the SMTP server requires SSL authentication.

Default: False

Note: Use SSL is supported for SMTP tests for SystemEDGE hosts only.

VRF Name

Specifies the VPN routing instance for the test (Ping and Traceroute for Cisco and Juniper test hosts).

Schedule a Test

The Schedule tab lets you schedule a test. Depending on which test you are configuring, you may or may not have access to the following Schedule parameters.

Schedule State

Enables and disables a test schedule.

Default: Disabled

Schedule Time Interval

Specifies the interval between scheduled test runs.

Default: 900 seconds

Schedule

Specifies one of the predefined schedules available from the drop-down list. For more information, see Create a Schedule (see page 49).

Default: 24/7

Note: Time zones for Schedule are local to the SpectroSERVER where the test host running the scheduled test is modeled.

Threshold Violation Interval

Specifies an alternate test interval that can be used during a threshold violation period. Decreasing the interval during a period of high latency can provide more precise data.

Default: 300 seconds

Note: If the Threshold Violation Interval is exceeded, the test does not resume until the Threshold Violation Interval is reached, a lower or higher value than the scheduled time interval.

Important! Setting this value too low can create additional traffic and load on the router during a period of high latency to make the situation worse.

Create a Schedule

You can create test schedules if the predefined schedules do not meet your particular requirements. The schedules that you create are not test-specific; they are available for all tests. For more information about creating schedules, see the *Operator Guide*.

Note: If you create a schedule with Recurrence set to None, the test runs once on the start date. Then the schedule reverts to the default schedule, and the new schedule is disabled.

Follow these steps:

1. Click Create in the Schedule tab.

   The Create Schedule dialog opens.

2. Configure schedule settings, and click OK.

   The new schedule appears in the Schedule drop-down list.

Specify Alarm Thresholds for a Test

The Threshold tab lets you configure alarm thresholds to monitor response time measurements on a specific link or path. Threshold parameters vary among tests. When a threshold value is exceeded, CA Spectrum generates an event, an alarm, or both, based on the settings you specify.

Threshold parameters depend on the type of test. The following list describes Threshold parameter options:

Active Thresholds Schedule

Specifies one of the predefined schedules during which thresholds are in effect and which is available from the list. You can use this feature to measure tests against thresholds only during certain times of the day. For more information, see Create a Schedule (see page 49).

Default: 24/7

Note: Time zones for schedules are local to the SpectroSERVER where the test host running the scheduled test is modeled.

Threshold Events Asserted On

Specifies the model from the list where events are asserted.

Threshold Types

Identifies threshold settings for the threshold types that are related to a test.

Status

Enables and disables each threshold type for a test.

Event

Specifies a response time threshold value (greater than 0) that, if exceeded, generates an event.

Depending on the threshold type, you can use one of the following standards to specify a threshold value:

- A time interval in milliseconds (ms)
- A percentage (%) of packet errors encountered

Minor Alarm

Specifies a response time threshold value (greater than 0) that, if exceeded, generates a minor alarm.

Depending on the threshold type, you can use one of the following standards to specify a threshold value:

- A time interval in milliseconds (ms)
- A percentage (%) of packet errors that were encountered

Major Alarm

Specifies a response time threshold value (greater than 0) that, if exceeded, generates a major alarm.

Depending on the threshold type, you can use one of the following standards to specify a threshold value:

- A time interval in milliseconds (ms)
- A percentage (%) of packet errors encountered

Critical Alarm

Specifies a response time threshold value (greater than 0) that, if exceeded, generates a critical alarm.

Depending on the threshold type, you can use one of the following standards to specify a threshold value::

- A time interval in milliseconds (ms)
- A percentage (%) of packet errors encountered

Threshold Cycles

Specifies a value (greater than 0) for the number of consecutive test cycles that violate the threshold before CA Spectrum generates an event or alarm.

Clear Threshold

Specifies a response time threshold value (greater than 0) tha,t if not exceeded, clears an event or alarm. Depending on the threshold type, you can use one of the following standards to specify a threshold value:

- A time interval in milliseconds (ms)
- A percentage (%) of packet errors encountered

Clear Cycles

Specifies a value (greater than 0) for the number of consecutive test cycles that comply with a threshold before CA Spectrum clears an event or alarm.

Establish Baseline Data to Determine Valid Thresholds

The threshold values to use for a test are often too high or too low. You can establish baseline response times that you can then use to determine appropriate thresholds.

Use the following procedure to determine valid thresholds for a test.

Follow these steps:

1. Schedule multiple test runs over the interval to which you want to apply thresholds to tests.
2. Analyze test result data to determine realistic performance thresholds. For more information, see Viewing Service Performance Manager Information (see page 65).
3. Configure test thresholds that are based on the results of your analysis.

Considerations for CA eHealth and Cisco IP SLA Tests

Service Performance Manager test scheduling is handled by the respective agent. The other management applications, such as CA eHealth, can discover the tests while providing an administrator a single point for RTM test configuration.

Cisco IP SLA tests only support a sample count of '1' for all test types other than Jitter. If a sample count other than 1 is used when configuring the test in Service Performance Manager, CA Spectrum schedules the test instead of the agent. This results in CA eHealth (and other management applications) not being able to discover the test, because CA eHealth only discovers tests that are scheduled by the agent.

The following test types describe the results that can be expected, if you specify a Sample Count value while configuring a test for a Cisco IP SLA agent:

- For all non-Jitter test types:
  - If Sample Count > 1, CA Spectrum schedules the test and CA eHealth (and other management applications) fails to discover the test.
  - If Sample Count == 1, CA Spectrum uses the agent to schedule the test and CA eHealth (and other management applications) discovers the test.
- For Jitter tests, CA Spectrum uses the agent regardless of the sample count and CA eHealth (and other management applications) discovers the test.

The Sample Count value is specified on the Advanced tab when configuring a test. For more information, see Configure Advanced Parameters (see page 45).

Run Tests on an On-Demand Basis

You can run tests manually on an on-demand basis if the following criteria are met:

- The test is not scheduled or is scheduled and the schedule is disabled.
- The test is enabled.
- The test host for the test is activated. See Activate and Deactivate Test Hosts (see page 53) for more information.

Typically you manually run tests for diagnostic purposes. For example, you can run an HTTP test to determine a web server response to requests, or you can run a Jitter test to determine the quality of VoIP transmission.

Follow these steps:

1. In the Explorer tab under Service Performance Manager, expand the Test Hosts folder.

   Available test hosts appear.

2. Select the test host.

   Available tests appear in the Test List table on the Information tab of the Contents panel.

3. Select the test(s) you want to run and click the Run Test icon.

   Information about the test is updated in the Test List table.

   Note: If the test information is not updated, click the Refresh icon.

   Test result information is available in the Component Detail panel.

   Note: To display the Component Detail panel from the Test List table, click the Information icon.

Activate and Deactivate Test Hosts

All test hosts are modeled in CA Spectrum in the active state. Tests can be configured on a test host in either the active or inactive state. However, tests can only be run on active test hosts.

Note: If the device model that is associated with a test host is in maintenance mode, an error is displayed and the test host is not activated. When the device model is taken out of maintenance mode, the test host is activated (if it was active when the device model went into maintenance mode).

Follow these steps:

1. In the Explorer tab under Service Performance Manager, expand the Test Hosts folder.

   The test hosts appear in the Contents panel on the List tab. The State field indicates whether test hosts are Active or Inactive.

2. In the Contents panel on the List tab, select the inactive test host(s) you want to activate, right-click the selection, and select Activate Test Host.

   The test host is activated.

3. To deactivate a test host, select the active test host(s) you want to deactivate, right-click the selection, and select Deactivate Test Host.

   Note: Any scheduled tests stop running until the test host is reactivated.

   The test host is deactivated.

Manage Tests

If you have the required privileges to the test, you can edit parameter settings and can delete any test. The administrative-user and read/write privileges are required to make modifications.

Important! Editing and deleting tests or test templates should be performed with caution by qualified personnel. This guidance especially applies in cases when, for example, Service Performance Manager performance test results are monitored by SLAs (service level agreements) that are modeled in CA Spectrum or when tests are run for infrastructure performance analysis.

Edit a Test

You can edit all test parameter settings as required.

When you edit a test, the test stops and restarts after all changes have been completed. As a result, the test schedule can be disrupted. For example, if a test has a 60-minute interval between scheduled runs and it is edited 58 minutes after the last scheduled run, it runs for 1 hour and 58 minutes after it is restarted.

Follow these steps:

1. Locate a test to edit. In the Explorer tab under Service Performance Manager, expand the Templates or Test Hosts folders.
2. Expand templates or test hosts.

   Available tests appear.
3. Right-click the test to edit, and select Edit Test.
4. Modify test parameters as required. For more information about configuration options, see Configure Service Performance Manager Tests (see page 39).

Delete a Test

When you delete a test, you remove it permanently from CA Spectrum.

Follow these steps:

1. Access the Explorer tab under Service Performance Manager.
2. Locate a test to delete by expanding the Templates or Test Hosts folders, and then templates or test hosts.

   Available tests appear.
3. Right-click the test to delete, and select Delete.

   The Confirm Delete dialog opens.
4. Click Yes.

   The test is deleted.

Chapter 4: Working with Test Templates

This section contains the following topics:

About Test Templates

A test template is a test configuration that you can apply to multiple test hosts in a single step to create tests on the test hosts. You configure and edit test templates the same way you do with tests. Where they are different is in their scope of application. When you create a test, you create it on a single test host. When you create a test template, however, you can apply it to multiple tests hosts in the following ways:

- Selectively apply a template to multiple test hosts that support the test that is specified by the template.
- Apply a template to any number of test hosts that support the tests that are specified by the templates and that are added to a Global Collection container.

Verify the following primary advantages of using a test template:

- You can implement automated bulk performance testing.
- All modifications to test template parameters are automatically applied to the tests on each test host to which the template is applied. For example, changing a threshold value in a template changes that threshold value for all tests that are derived from it.
- A test template allows you to specify that a test is either a test host or a destination type. A test host type specifies a variable test host but a constant destination. A destination type specifies a constant test host but variable destinations.

Create Test Templates

You can create performance test templates using either of the following methods:

- Create a test template from scratch
- Save a different version of an existing test template

You can use any method to create a test template. For more information, see Configure Service Performance Manager Tests (see page 39). You can also configure the following template-specific parameters:

Template Type

Specifies Test Host or Destination. A test host type specifies a variable test host with a constant destination. A destination type specifies a constant test host with variable destinations. (The Destination configuration is not available for DHCP and HTTP test templates.)

Global Collections

(Optional) Specifies one or more Global Collection containers. OneClick automatically applies the test that is specified by the template to all test hosts that you add to the container if they support the test.

Create a New Test Template

You can create a test template from scratch. Use this method to create a test template if no other templates have been created.

Follow these steps:

1. In the Explorer tab under Service Performance Manager, right-click Templates, select Create Test Template, and select a test type.

   The Create Test Template dialog provides test template parameters. You can specify the Template type and one or more Global Collection containers to which to apply the template.

2. Configure test template settings, and click OK.

   The new template is saved and appears in the Templates folder.

3. For information about the new test template, select the new template.

   Information appears in the Information tab in the Contents panel.

Create a Different Version of an Existing Test Template

You can create a test template from a copy of another template.

Note: You cannot copy test templates between domains where different versions of CA Spectrum are running.

Follow these steps:

1. In the Explorer tab under Service Performance Manager, expand the Templates folder.

   The test templates appear.

   Note: If no templates appear, create a test template (see page 58).

2. Right-click the test template to copy, and select Copy Test Template.

   The Copy Test Template dialog lets you select settings for the new template.

   Note: The test templates that you copy are disabled by default, and "_COPY" is appended to the test name. You can rename the template.

3. Modify test template settings, and click OK.

   The new template is saved and appears in the Templates folder.

4. (Optional) Select the new template.

   Information appears in the Information tab in the Contents panel.

Apply a Test Template to Test Hosts

You can selectively apply a test template to a group of test hosts that support the template test type. Or you can automate the process by placing test hosts in a Global Collection container and applying a test template to the container. Apply a test template to a Global Collection container so that tests are automatically created for all test hosts that support the test type as they are added to the container. For more information, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Selectively Apply a Test Template to One or More Test Hosts

You can manually apply a test template to a selection of test hosts. You can precisely specify only those test hosts for which you want to create tests.

Follow these steps:

1. In the Explorer tab under Service Performance Manager, select the Templates folder.

   The test templates appear in the Contents panel on the List tab.

   Note: If no templates appear, create a template. For more information, see Create a New Test Template (see page 58).

2. In the Contents panel on the List tab, select the template(s) to apply.
3. Right-click the selection, and select Apply Test Template.

   The Select Test Host dialog lists test hosts that support the template test type.
4. Select one or more test hosts to which to apply the test template, and click OK.

   OneClick creates the test for the selected test hosts. The tests that were created from the template appear beneath the template in the Explorer tab.

   Note: The List tab in the Contents panel also lists tests that were created from a test host template type when the template is selected.

   Two naming formats are supported for tests that were created from test templates. The test names can indicate the test target IP address, or they can indicate the test target model name. The target can be the test host or a particular device, depending on the template type.

   Use the following default format:

   ```
   Template Name_IP Address
   ```

   Template Name

   Specifies the name of the template that you applied to a test host.

   IP Address

   Specifies the IP address for the test target.

   You can use the SPM Template Naming option from the OneClick Administration Pages to change the naming convention to the following format:

   ```
   Template Name_Model Name
   ```

   Template Name

   Specifies the name of the template that you applied to a test host.

   Model Name

   Specifies the model name for the test target.

   The SPM Template Naming setting does not change the naming format for tests that have already been created from a template.

Apply a Test Template to a Global Collection Container

Applying test templates to Global Collection containers lets you automate the process of creating tests of different types for multiple test hosts. For example, assume a Global Collection container includes a group of test hosts that only supports ICMP Ping tests, a group that only supports HTTP tests, and a group that supports both. Assume also that numerous test hosts that belong to each group are sometimes added to the container.

In this case, two different test templates can be applied to the container to create the tests for the test hosts that are included in it. One template specifies an ICMP Ping test and the other specifies an HTTP test. ICMP Ping tests are created for the test hosts that support ICMP Ping tests, and HTTP tests are created for the test hosts that support HTTP tests.

This example understates the potential complexity of a “real-life” performance testing implementation. However, it does illustrate the ease with which you can use test templates to set up tests on multiple test hosts. This method is an alternative to setting them up individually. For a more information, see Example Implementation Scenario (see page 61).

Follow these steps:

1. In the Create Test Template, Copy Test Template, or Edit Test Template dialog, click the Browse button next to the Global Collection parameter.

   The Select Collections dialog opens.

2. Select the Global Collections to which to apply the template, and click OK. If you prefer to create a Global Collection for your test hosts, take the following steps:

   a. Click Create.

   b. Select settings for the new Global Collection.

   c. Proceed with the selection process.

Example Implementation Scenario

This section illustrates how test templates can be applied to a Global Collection to implement automated bulk performance testing between a central office location and branch office locations.

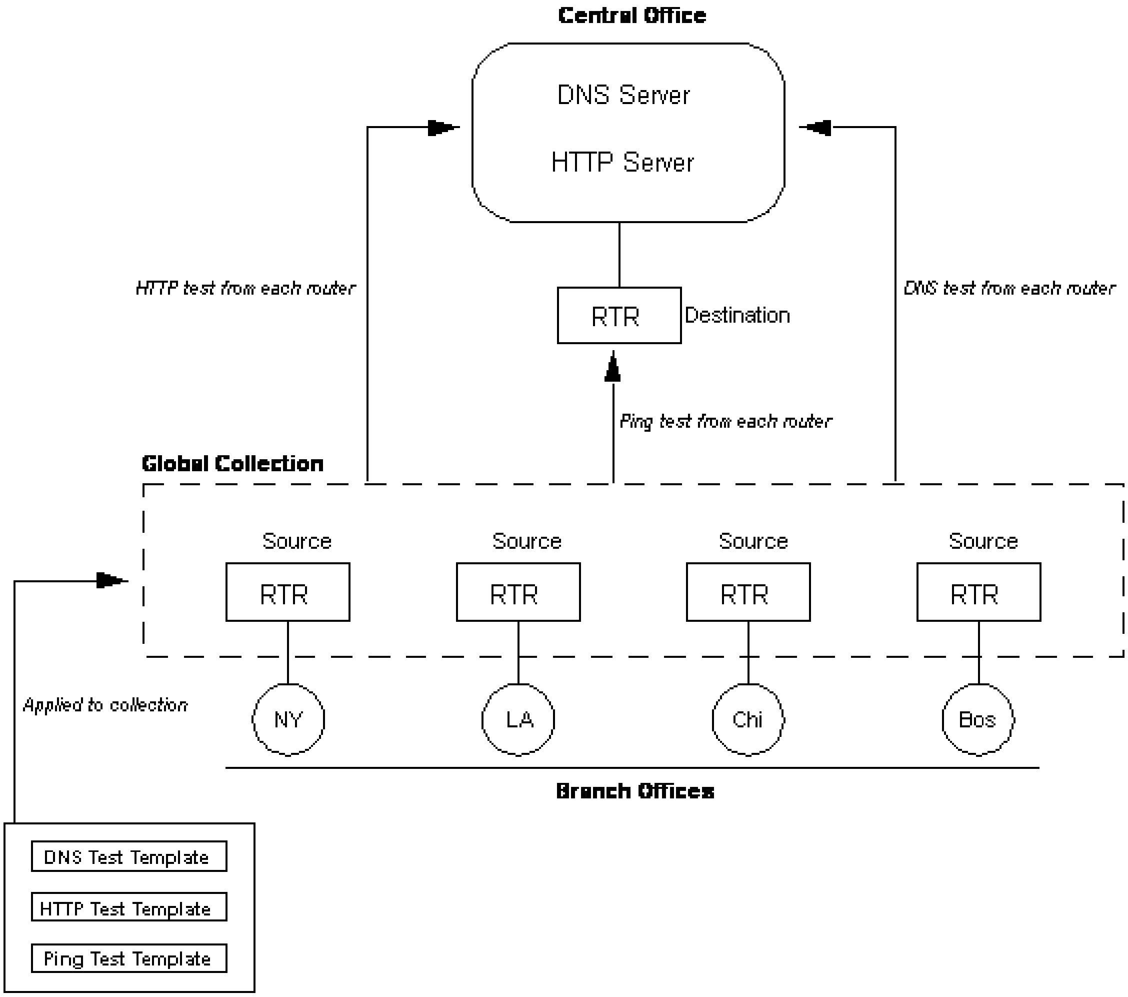
Scenario

- The central location of an organization provides domain name lookup and web services to numerous remote branch locations that connect to the central location on an intermittent basis.
- You can confirm that remote connections to the central location are maintained and the remote branch locations have continuous access to DNS and HTTP services that are provided by the central location.
- To determine whether service delivery from the main location to the remote locations remains viable, run Ping, DNS, and HTTP tests from remote location edge routers (that support the tests) on a regularly scheduled basis whenever they are brought online (connect to the central location edge router).
- Create a Global Collection that is configured to include all edge router models for remote locations as they are brought online.

- Three test templates are applied to a Global Container:
  - An ICMP Ping test template that is configured to create a Ping test on remote-location edge routers that tests connectivity to the central-location router.
  - A DNS test template that is configured to create a DNS lookup test on remote-location edge routers that tests DNS lookup time from the DNS server at the central location.
  - An HTTP test template that is configured to create an HTTP download test on remote-location edge routers that tests the round-trip time to download a web page from the HTTP server at the central location.

Test Template Scenario

The following image illustrates the example scenario.



About Destination Template Types

Test templates can use the Test Host or the Destination template. A Test Host template specifies a variable test host with a constant destination. A Destination template specifies a constant test host with variable destinations.

When applying a Destination test template to Global Collections, CA Spectrum populates the Destination Address from the type of model to which the test template is applied. Both port and device models are supported as destinations. These models must exist in or must be added to the target Global Collection for the test template to be applied.

Device models

> When a Destination template is applied to a device model, the network address of the device is used as the Destination Address.

Port models

> When a Destination template is applied to a port model, the IP address of the port is used as the Destination Address.

The Destination Address can be modified after the test is created.

Manage Test Templates

When you edit a template, all the tests that are created from the template are updated with the modified settings. When you remove the association between a template and a Global Collection or delete a template, all tests that are created from the template are deleted.

Important! Editing and deleting tests or test templates should be performed with caution by qualified personnel. This guidance especially applies in cases when, for example, Service Performance Manager performance test results are monitored by SLAs (service level agreements) that are modeled in CA Spectrum or when tests are run for infrastructure performance analysis.

Edit a Test Template

You can edit all test template parameter settings as required. The changes apply to all tests that you created with the template. You can also remove the association between a template and a Global Collection when you edit a template.

Note: You can remove the association between a template and a Global Collection. Delete the value of the Global Collections parameter in the Edit Test Template dialog. When you remove the association, all tests on the test hosts in the collection are deleted.

Follow these steps:

1. In the Explorer tab under Service Performance Manager, expand the Templates folder.

   The test templates appear.

   Note: If no templates appear, create a template. For more information, see Create a New Test Template (see page 58).

2. Right-click the test template that you want to edit and select Edit Test Template.

   The Edit Test Template dialog opens.

3. Modify the template settings and click OK.

   The changes are applied to the template and to all tests that are created from it.

Delete a Test Template

When you delete a template, you also delete all tests that are created from that template.

Follow these steps:

1. In the Explorer tab under Service Performance Manager, expand the Templates folder.

   The test templates appear.

2. Right-click the test template that you want to delete and select Delete.

   A confirmation dialog opens.

3. Click Yes.

   The test template is deleted.

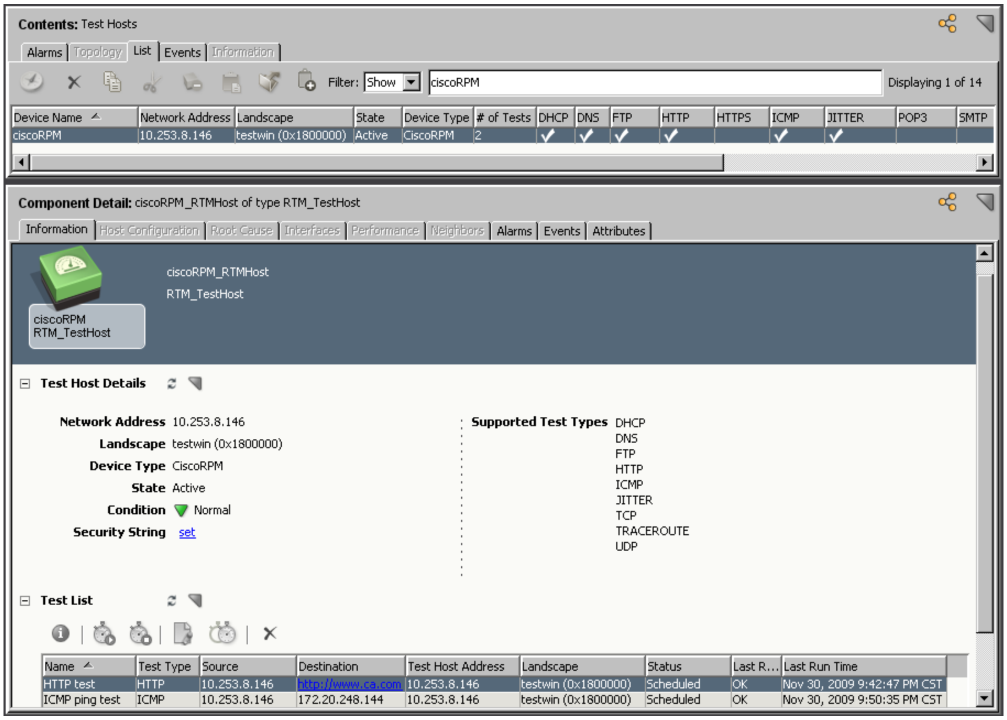
Chapter 5: Viewing Service Performance Manager Information

This section contains the following topics:

Test Host Information

The OneClick Console displays summary and detailed information about test hosts that are modeled in CA Spectrum and lets you perform operations on tests for test hosts. OneClick provides views of test hosts, test templates, tests, and test results. You can also see detailed information about events and alarms for Service Performance Manager components.

The following image shows an example view of a test host:



Contents: Test Hosts

Filter: Show ciscoRPM Displaying 1 of 14

Device Name	Network Address	Landscape	State	Device Type	# of Tests	DHCP	DNS	FTP	HTTP	HTTPS	ICMP	JITTER	POP3	SMTP
ciscoRPM	10.253.8.146	testwin (0x1800000)	Active	CiscoRPM	2	✓	✓	✓	✓		✓	✓		

Component Detail: ciscoRPM_RTMHost of type RTM_TestHost

ciscoRPM_RTMHost
RTM_TestHost

Test Host Details

Network Address 10.253.8.146
Landscape testwin (0x1800000)
Device Type CiscoRPM
State Active
Condition Normal
Security String set

Supported Test Types DHCP
DNS
FTP
HTTP
ICMP
JITTER
TCP
TRACEROUTE
UDP

Test List

Name	Test Type	Source	Destination	Test Host Address	Landscape	Status	Last R...	Last Run Time
HTTP test	HTTP	10.253.8.146	http://www.ca.com	10.253.8.146	testwin (0x1800000)	Scheduled	OK	Nov 30, 2009 9:42:47 PM CST
ICMP ping test	ICMP	10.253.8.146	172.20.248.144	10.253.8.146	testwin (0x1800000)	Scheduled	OK	Nov 30, 2009 9:50:35 PM CST

Click Refresh in a OneClick view to see current information. You can refresh and customize views and dock and undock panels. You can set up table column preferences to display only the information types that you want to view. For more information, see the *Operator Guide.*

The Contents panel displays information about the selected test host model, the landscape where it is modeled, its state (Active or Inactive), and the test types that it supports. From the Contents panel, you can create tests for the test host, discover tests for the test host, and activate and deactivate the test host.

More information:

Finding Components (see page 21)

Test Host Information in the Component Detail View

The Component Detail panel provides detailed information about a selected test host. The Information tab of the Component Detail panel includes two categories of information about the test host:

Test Host Details

Provides detailed information about the test host and lets you set the test host model security string.

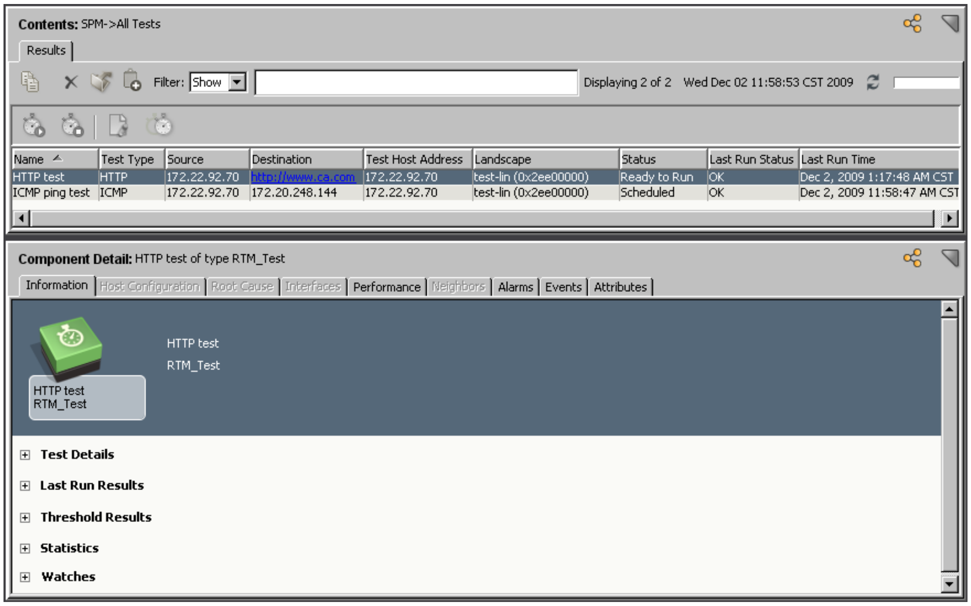
Test List

Displays information about tests for the selected test host. It also lets you run tests, stop tests, manage tests, and invoke the Component Detail view for tests.

Note: For information about accessing information about alarms and events for Service Performance Manager components, see Alarms and Events (see page 70).

Test Information

OneClick Console displays summary and detailed information about tests that are modeled in CA Spectrum and lets you perform operations on tests. The following image shows an example view.



Contents: SPM->All Tests

Results

Filter: Show

Displaying 2 of 2 Wed Dec 02 11:58:53 CST 2009

Name	Test Type	Source	Destination	Test Host Address	Landscape	Status	Last Run Status	Last Run Time
HTTP test	HTTP	172.22.92.70	http://www.ca.com	172.22.92.70	test-lin (0x2ee00000)	Ready to Run	OK	Dec 2, 2009 1:17:48 AM CST
ICMP ping test	ICMP	172.22.92.70	172.20.248.144	172.22.92.70	test-lin (0x2ee00000)	Scheduled	OK	Dec 2, 2009 11:58:47 AM CST

Component Detail: HTTP test of type RTM_Test

The Contents panel table displays information about the selected test model, the landscape where it is modeled, the IP addresses of the test source, test destination, and test host for the test. It also provides additional information, such as the tests that are scheduled, running, or stopped, the last time the test was run, and the resulting status of the test (did or did not violate a threshold). Command icons for running, stopping, and managing tests are provided too.

Test Information in the Component Detail Panel

The Information tab in the Component Detail panel provides detailed information about a selected test:

Test Details

Provides information about test configuration settings, including scheduling and test threshold settings.

Last Run Results

Provides information about the most recent test run, including test results such as latency and packet loss values. Reported metrics vary depending on test host and test type.

Threshold Results

Provides information about threshold violations (event, minor, major, critical) resulting from the test. Threshold types vary depending on test host and test type.

Note: Regarding the sample count and the % of Threshold values, RTTMON can perform more than the repetitions that are specified for a test. Service Performance Manager includes this count in the results and calculates the average, maximum, and minimum results for latency and packet loss. Therefore, the value for percentage of packet loss can be other than a multiple of (1 / sample count) * 100.

For example: If you set sample count to 5, typically the percentage of packet loss is a value of 0%, 20%, 40%, ...100%. If the agent performs more than 5 repetitions, you can see 0%, 16.66%, 33.33%, ...100%.

Statistics

Provides statistical test result information for tests that are run for SystemEDGE test hosts.

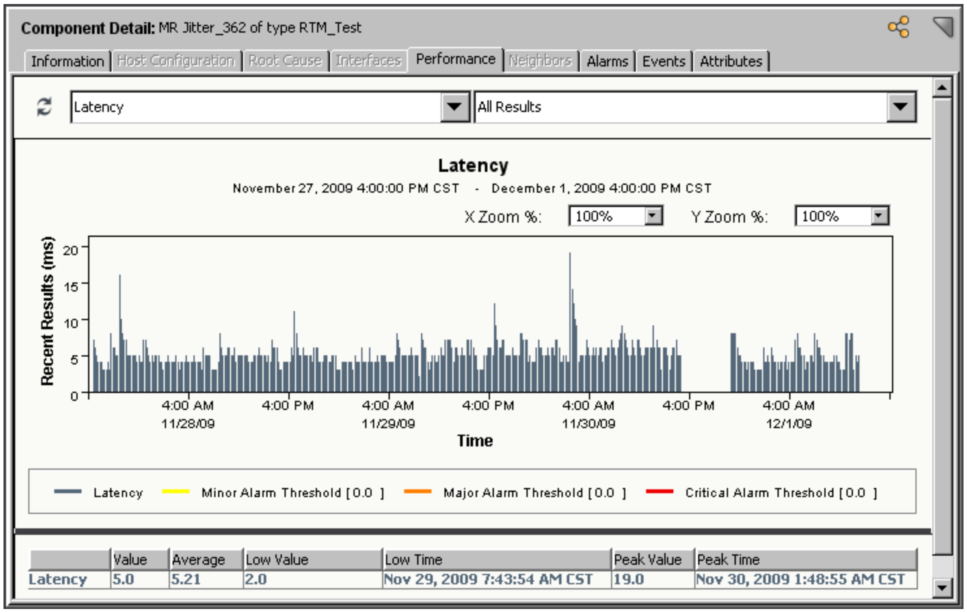
Note: This section appears for tests that are created for SystemEDGE test hosts only.

Watches

Provides information about any watches that have been defined on the test model.

Test Performance Information in the Component Detail Panel

The Performance tab in the Component Detail panel shows graphical representations of test results. The following image shows an example test performance graph.



Component Detail: MR Jitter_362 of type RTM_Test

	Value	Average	Low Value	Low Time	Peak Value	Peak Time
Latency	5.0	5.21	2.0	Nov 29, 2009 7:43:54 AM CST	19.0	Nov 30, 2009 1:48:55 AM CST

Note: The Archive Manager for the test landscape must be running for Service Performance Manager to display performance test results.

Specify the Interval

You can specify the following time intervals for which you want to display performance results:

- 1 hour
- 3 hours
- 6 hours
- 12 hours
- 1 Day
- 1 Week
- 4 Weeks
- All Results

Note: The All Results option retrieves all result data that is stored in the CA Spectrum Distributed Data Manager (DDM) database, up to a maximum of 365 days. By default, the DDM stores up to 45 days of data. See the *Database Management Guide* for more information.

Important! Retrieving large numbers of events can affect performance.

To specify the interval, select an interval from the list.

View Test Data

You can view data from a selected data point in a graph.

To view test data, position your mouse pointer over the end of a data point line in the graph. A descriptive label (including date, time, and value) is displayed for that data point.

You can also view additional test data (averages, high and low values) in tabular form under the graph.

Adjust an Axis

You can adjust the dimensions of the X and Y axes as necessary to meet your viewing requirements. For example, you can adjust the X axis to display latency outliers that are not visible from the default view.

To adjust the dimension of an axis, select a zoom percentage from the list for the X or Y axis, or supply a value.

Note: 100% is the minimum allowable zoom percentage.

Timeout Data Setting Affects a Performance Graph

When you configure a test, you can specify that data generated as a result of a test timeout is filtered out of test results. This setting is enabled by default. Timeouts and test failures can cause gaps in the graph. When timeout filtering is enabled, you cannot discern these gaps. Examples of test failures include lost contact to device, device in maintenance mode, or device failure.

A setting of False, however, causes the following effects:

- Skewed performance graph auto-scaling: Timeout values can so greatly exceed the response time values that exact response times on the performance graph can be difficult to discern.
- Skewed average calculation: Timeout values can so greatly exceed response times that average calculations are inaccurate.
- Skewed data from data export: Timeout values can be prevalent in the exported data. As a result, depending on your post-processing mechanisms, results can be undesirable.

Alarms and Events

You can view alarms for Service Performance Manager components from multiple points in the OneClick Console. Use the Explorer tab to view events and alarms for Service Performance Manager components.

Follow these steps:

1. Select Service Performance Manager in the Explorer tab and click the Alarms tab in the Contents panel.

   All alarms related to Service Performance Manager events appear in the Alarms tab.

2. Select an alarm in the Contents panel.

   The Alarm Details and Events tabs in the Component Detail panel display detailed information for the selected alarm.

You can also view events and alarms for Service Performance Manager components from the Locater tab.

Follow these steps:

1. List the components whose event and alarm information you want to view. For more information, see Finding Components (see page 21).
2. In the Contents panel, select a component.
3. In the Component Detail panel, click the Alarms or Events tab to view information.

Chapter 6: Generating Reports on Test Data

This section contains the following topics:

Service Performance Manager Reports from Report Manager

CA Spectrum provides the following options for reporting and reviewing performance test results:

CA Spectrum Report Manager

Lets you generate summarized and detailed performance test results in various text and graphical formats on an on-demand or scheduled basis.

Externalized Result Data

Lets you use the Service Performance Manager result data that has been compiled over an extended period and is exported to text files.

Service Performance Manager report options are included under the Response Time report pack in Spectrum Report Manager. Spectrum Report Manager provides numerous options for customizing report content, format, and organization. For more information, see the *Spectrum Report Manager User Guide*.

Report Manager Options

Spectrum Report Manager provides following options for generating and managing your round-trip time (RTT) reports:

- Generate reports on demand. Use this option to generate the most recent RTT test results.
- Schedule RTT test report generation on a one-time or periodic basis.
- Specify how long you want Spectrum Report Manager to retain scheduled RTT test reports or how many reports to retain.
- Specify email recipients for scheduled RTT test reports.
- Schedule RTT test reports for other Spectrum Report Manager users.
- Publish RTT test reports in PDF, text, and spreadsheet formats. Use the documents for briefings and presentations on network performance issues.

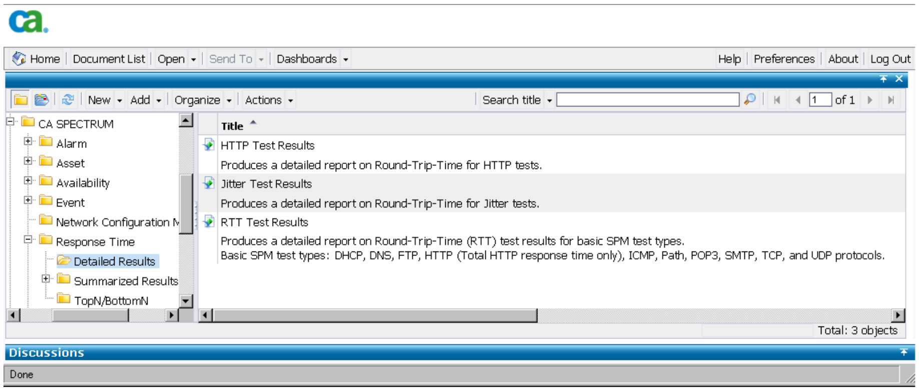
How to Generate Performance Reports with Report Manager

You can generate performance reports on demand or schedule reports with Spectrum Report Manager.

Follow these steps:

1. Select the type of test you want to generate.

   The following image shows the Service Performance Manager report options:



HTTP Test Results

Produces a detailed report on Round-Trip-Time for HTTP tests.

Jitter Test Results

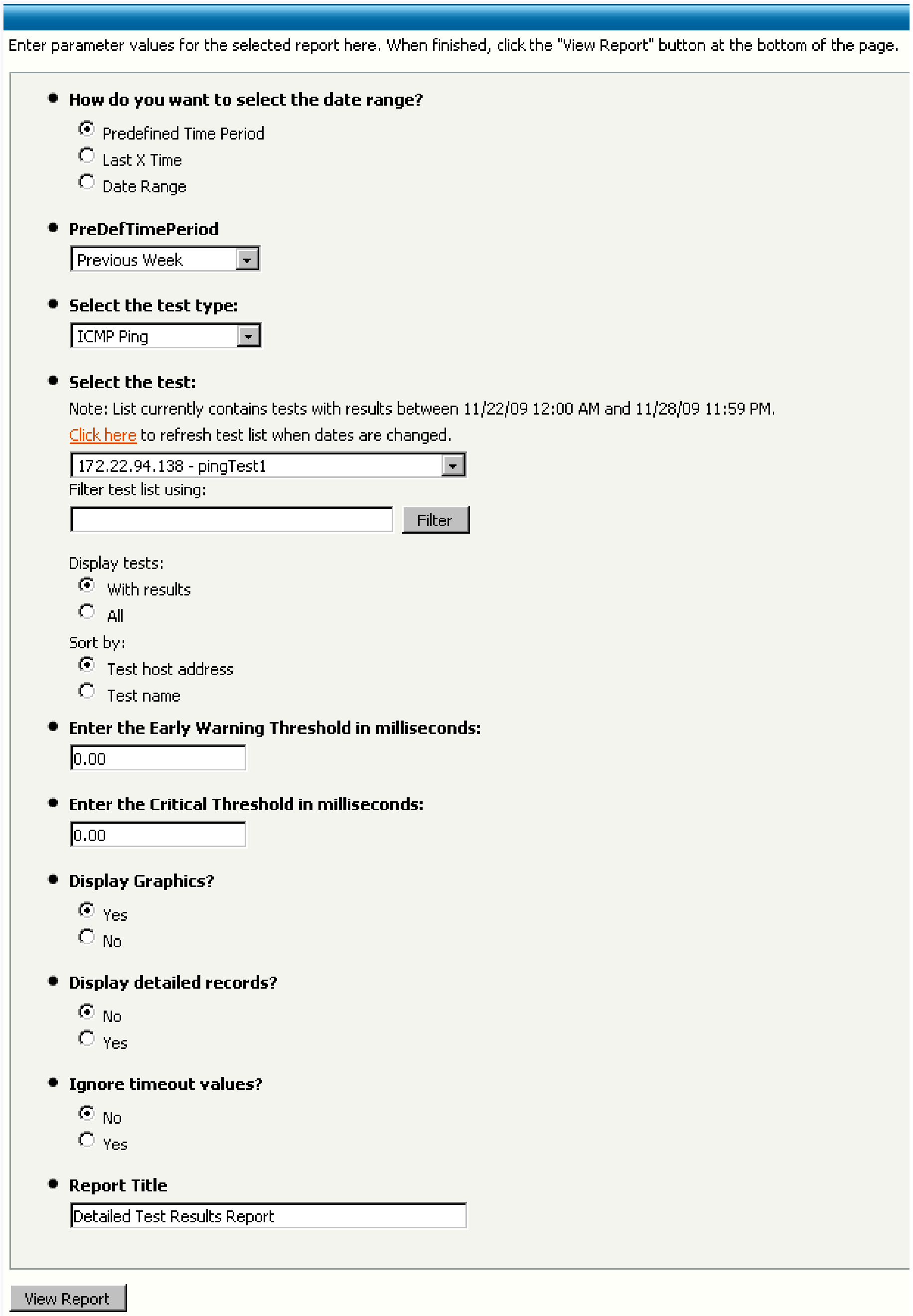
Produces a detailed report on Round-Trip-Time for Jitter tests.

RTT Test Results

Produces a detailed report on Round-Trip-Time (RTT) test results for basic SPM test types.
Basic SPM test types: DHCP, DNS, FTP, HTTP (Total HTTP response time only), ICMP, Path, POP3, SMTP, TCP, and UDP protocols.

2. Configure the report.

The following image shows an example of a configuration page for an ICMP Ping report:



Enter parameter values for the selected report here. When finished, click the "View Report" button at the bottom of the page.

- **How do you want to select the date range?**

  ● Predefined Time Period
  ○ Last X Time
  ○ Date Range

- **PreDefTimePeriod**

  Previous Week

- **Select the test type:**

  ICMP Ping

- **Select the test:**

  Note: List currently contains tests with results between 11/22/09 12:00 AM and 11/28/09 11:59 PM.
  Click here to refresh test list when dates are changed.

  172.22.94.138 - pingTest1

  Filter test list using:

  Filter

  Display tests:
  ● With results
  ○ All

  Sort by:
  ● Test host address
  ○ Test name

- **Enter the Early Warning Threshold in milliseconds:**

  0.00

- **Enter the Critical Threshold in milliseconds:**

  0.00

- **Display Graphics?**

  ● Yes
  ○ No

- **Display detailed records?**

  ● No
  ○ Yes

- **Ignore timeout values?**

  ● No
  ○ Yes

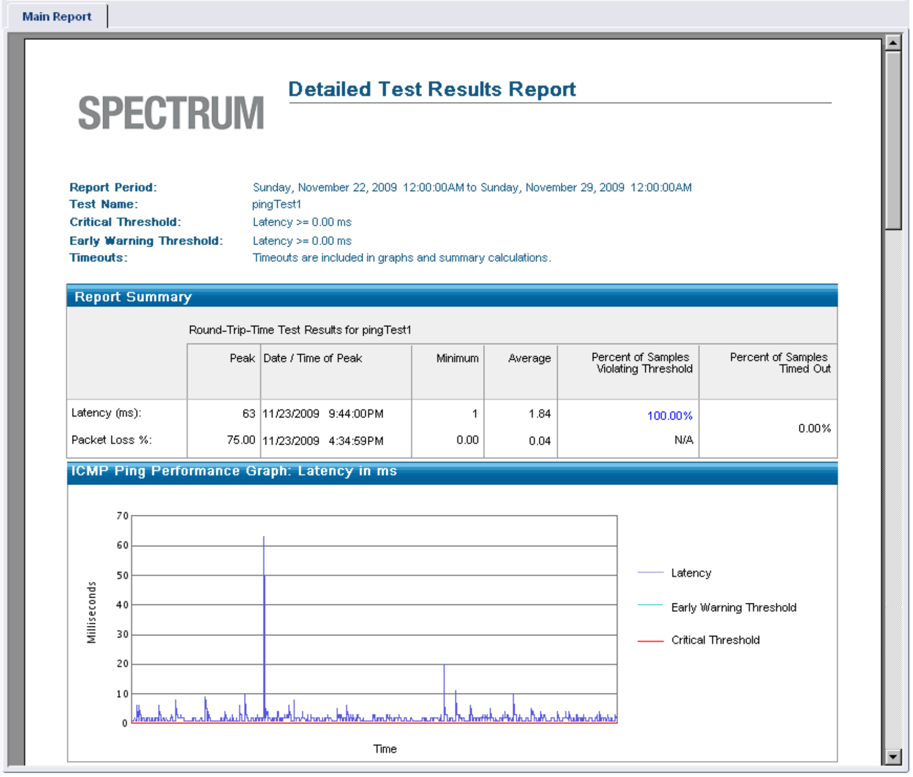
- **Report Title**

  Detailed Test Results Report

View Report

3. Click View Report to generate the report.

   The generated report displays. The following image shows a portion of the report results:



Detailed Test Results Report

Report Period: Sunday, November 22, 2009 12:00:00AM to Sunday, November 29, 2009 12:00:00AM
Test Name: pingTest1
Critical Threshold: Latency >= 0.00 ms
Early Warning Threshold: Latency >= 0.00 ms
Timeouts: Timeouts are included in graphs and summary calculations.

Report Summary

Round-Trip-Time Test Results for pingTest1

	Peak	Date / Time of Peak	Minimum	Average	Percent of Samples Violating Threshold	Percent of Samples Timed Out
Latency (ms):	63	11/23/2009 9:44:00PM	1	1.84	100.00%	0.00%
Packet Loss %:	75.00	11/23/2009 4:34:59PM	0.00	0.04	N/A	

ICMP Ping Performance Graph: Latency in ms

4. Using View and manage report results, you can page through the report and search for text, email, and print the report.

Service Performance Manager Result Data

You can export Service Performance Manager result data that is compiled over an extended period using the SPM result logger. SPM result logger output files include a model handle, timestamp, and a list of test-specific results per line. Once logging is enabled, Service Performance Manager produces text files with result data in SSLogger format. All result files are created and saved in an output directory that you create. New log files are created after an interval that you specify. For information about configuring data export parameters, see the *Administrator Guide*.

Data Logging Event Codes

The following table lists Service Performance Manager data logging event codes:

Event Code	Event	Contains Statistics For...
0x04560000	SPM Result Event	Latency and packet loss (DHCP tests, which do not contain data for packet loss, are not included.)
0x0456002e	SPM Result Event (HTTP)	HTTP response time, DNS resolution time,TCP connect time, and HTTP download time
0x04560010	SPM Result Event (Jitter)	Jitter response time, Jitter source to destination time, Jitter destination to source time, Jitter MIA, Jitter late arrival, and Jitter busies
0x0456003e	SPM Result Event (Traceroute)	Latency

Result Events

For SPM result events, the preceding data is followed by statistical data particular to the RTM_Test. The event code dictates which of the statistics are relevant.

Note: Irrelevant statistics for a given test type (for example, Jitter statistics for a ping test) are reported as 0.

The remaining 12 reported statistics in a logged event correspond to, in order:

- Latency
- Packet loss
- HTTP response time
- DNS resolution time
- TCP connect time
- HTTP download time
- Jitter response time
- Jitter source to destination time
- Jitter destination to source time
- Jitter MIA

- Jitter late arrival
- Jitter busies

Data Export Sample

The following sample illustrates the structure of logged Service Performance Manager test result data:

```
0x830201d,6PM-7AM_6.6.0.2,1054176719,0x4560000,1,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
0x8302010,Jitter_6.6.0.2,1054176724,0x4560010,0,0.0,0,0,0,0,5,0.0,0.0,0.0,0.0,0.0
0x8302012,FTP_6.6.0.2,1054176730,0x4560000,843,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
0x8302017,TCP_6.6.0.2,1054176748,0x4560000,1,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
0x830201b,24x7_6.6.0.2,1054176767,0x4560000,1,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
0x6a00f8a,TCP_6.6.0.0,1054176941,0x4560000,6,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
0x6c009de,Traceroute_6.6.0.1,1054176872,0x456003e,40,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
0x6c009d6,FTP_6.6.0.1,1054176872,0x4560000,858,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
0x6c009e0,TCP_6.6.0.1,1054176872,0x4560000,12,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
0x8302011,HTTP_6.6.0.2,1054176837,0x456002e,0,0.0,753,5,32,716,0,0.0,0.0,0.0,0.0,0.0
0x830201f,6-11M-F_6.6.0.2,1054176870,0x4560000,1,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
0x6c009e6,24x7_6.6.0.1,1054176927,0x4560000,5,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
0x6c009e8,6PM-7AM_6.6.0.1,1054176937,0x4560000,5,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
0x6c009d5,HTTP_6.6.0.1,1054176939,0x456002e,0,0.0,19,0,7,12,0,0.0,0.0,0.0,0.0,0.0
0x6a00f8b,ICMP_6.6.0.0,1054177035,0x4560000,1,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
0x6c009df,UDP_6.6.0.1,1054176943,0x4560000,3,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
0x8302019,UDP_6.6.0.2,1054176906,0x4560000,7,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
0x6c009eb,6-11M-F_6.6.0.1,1054176960,0x4560000,8,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
0x6c009dd,ICMP_6.6.0.1,1054176978,0x4560000,4,0.0,0,0,0,0,0,0.0,0.0,0.0,0.0,0.0
```

Test Modification Event

Service Performance Manager test modification events (event code 0x0456000a) contain the following statistical data, in addition to the common data described in Data Logging Event Codes (see page 77):

- Test name
- Destination address
- Packet size
- Source address
- Test interval
- Sample count

Chapter 7: Using the Command Line Interface (CLI) to Manage Tests

This section contains the following topics:

Overview: CLI Response-Time Testing

Response time tests are represented in CA Spectrum as models of model type RTM_Test. You can use the CA Spectrum Command Line Interface (CLI) to create, run, and edit response time tests and get test results as an alternative method to using the user interface in OneClick. For more information, see Working with Performance Tests (see page 27). You can issue test management commands from the CLI command line, or you can embed CLI commands in scripts, which you can run on an ad hoc or scheduled basis.

Important! Before you attempt to create and manage tests with the CLI, understand Service Performance Manager concepts, CLI commands and command syntax, and CA Spectrum modeling concepts.

Using the following CLI commands, you can create and manage tests:

- ack alarm
- connect
- create
- current
- destroy
- disconnect
- jump
- seek
- setjump
- show
- stopShd
- update

For more information, see the *Command Line Interface User Guide.*

Create Tests in CLI

You can create any of the response time test models that CA Spectrum supports using the CLI create command. For more information, see Required Parameters for Creating Tests (see page 83).

The following example script shows how to create a regularly scheduled Ping test. It enables a latency threshold, a latency value that, if exceeded, triggers a minor alarm, and a latency value that, if not exceeded, triggers an alarm clear.

```
#!/bin/ksh

cd $SPECROOT/vnmsh
connect
./create model mth=0x4560000 \
attr=0x1006e,val="Ping_Test_1" \ # Test Name
attr=0x4560005,val=0 \ # Test Type is ICMP_Ping
attr=0x45600f1,val=10.253.9.8 \ # TestHost address
attr=0x456001f,val=10.253.9.12 \ # Destination IP
attr=0x4560022,val=1 \ # Schedule is enabled
attr=0x4560014,val=600 \ # Test interval is 10 minutes
attr=0x4560035,val=1 \ # Latency Threshold is enabled
attr=0x456009b,val=100 \ # Latency Minor Threshold Set value
attr=0x4560017,val=100 \ # Latency Threshold Clear value
attr=0x4560027,val=2 # Clear Cycles
```

The following example script shows how to create an HTTP test. Note the formatting that is required for URL values.

```
#!/bin/ksh

cd $SPECROOT/vnmsh
connect
./create model mth=0x4560000 \
attr=0x1006e,val="Http_Test_1" \ # Test Name
attr=0x4560005,val=5 \ # Test Type is HTTP
attr=0x45600f1,val=10.253.9.8 \ # TestHost address
attr=0x456000f,val="http:\/\/www.ca.com\/about.htm" # Destination URL
attr=0x456008d,val="http:\/\/proxyServer" # Proxy URL
attr=0x4560022,val=1 \ # Schedule is enabled
```

Discover Tests in CLI

You can use the CLI update command to run SPM Test Discovery to discover and model performance tests that have been configured on test hosts but not with Service Performance Manager. Specify the discover tests action code (0x4560007) and the test host model handle. The following example script shows how to run SPM Test Discovery for a single test host.

Note: For more test action codes, see Test Action Codes (see page 110).

```
#!/bin/ksh

# this will discover tests for the test host with the given model handle.

cd $SPECROOT/vnsmh
connect
./update action=0x4560007 mh=<testhostMH>
```

Run Tests in the CLI

You can run a response-time test using the CLI update command. Specify the run test action code (0x4560009) and the test model handle. For more information, see Test Action Codes (see page 110).

The following example script shows how to run a single test. You can run multiple tests by specifying multiple tests in the script.

```
#!/bin/ksh

# this will run a test with the given model handle.

cd $SPECROOT/vnsmh
connect
./update action=0x4560009 mh=testMH
```

Edit Tests in the CLI

You can edit a response time test using an update command in the CLI. Change the values of test parameters by specifying new parameter values and issuing an update test action code (0x4560008).

The following example script shows how to modify a test schedule interval and test timeout values.

```
#!/bin/ksh

# change the schedule interval from 15 minutes to 30 minutes (1800 seconds)
# change the test timeout from 5000 ms to 1000 ms
# have the test not filter its timeout data

cd $SPECROOT/vnmsh
connect
./update mh=<testMH> attr=0x4560014,val=1800
./update mh=<testMH> attr=0x4560025,val=1000
./update mh=<testMH> attr=0x45600d6,val=FALSE
./update action=0x4560008 mh=$i
```

Get Test Results in the CLI

You can get various test status indications and test results using the CLI show command. This command also returns the parameters with the values that you want.

The following example script shows how to get test status and test results. For more information, see Test Status and Test Results Parameters (see page 110).

```
#!/bin/ksh

# obtain the latestResult status and latency/packet loss values for a given test

cd $SPECROOT/vnmsh
connect
./show attributes -e attr=0x4560004 attr=0x4560015 attr=0x456007d mh=<testMH>
```

Test Parameters Used in the CLI

The topics in this section list and describe parameters for creating and scheduling tests and setting test thresholds. You can configure RTM_Test model parameters using the user interface in OneClick. For more information, see Configure Tests (see page 39).

Parameters for Creating Tests

Required Parameters

For All Test Types

The following parameters are required for all response time tests:

Model_Name (0x1006e)

Specifies the name of the test. Only one test per host can exist with the same name. Duplicate test names are appended with "_COPY".

Test_Type (0x4560005)

Specifies the type of test to create. Once a test is created, this value cannot be changed. If it is changed, it is reset when the update takes place.

0 = ICMP

1 = UDP

2 = Trace Route

3 = TCP

4 = DNS

5 = HTTP

6 = POP3

7 = DHCP

8 = FTP

9 = SMTP

10 = Jitter

13 = Custom

14 = SQL Query

Default: None

Test_Host_Address (0x45600f1)

Specifies the IP address of a test host. This address must match the network address of the associated device model. Once a test is created, this value cannot be changed. If the value changes, it is reset when the update takes place.

For Specific Test Types

The following parameters are required when creating certain response time tests, depending on the test type:

Connect_String (0x456010a)

Specifies a string of commands to connect to the database. This parameter is required for some SQL Query tests, depending on database type.

Example:

```
jdbc:mysql://172.22.246.43/mysql?user=root&password=root
```

Database_Name (0x4560108)

Specifies the name of the database. This parameter is required for some SQL Query tests, depending on the database type.

Database_Type (0x456010b)

Specifies the type of database to test. This parameter is required for SQL Query tests. Correct drivers must be installed on the SystemEDGE computer.

0 = Oracle

1 = Microsoft SQL

2 = Other

Dest_File_Name (0x456000d)

Specifies the destination filename. This parameter is required for FTP tests.

Dest_Host_Name (0x456000a)

Specifies the destination test hostname. For DNS tests, it is the lookup name; for FTP and POP3 tests, it is the address where the transaction is performed. For Custom tests, it is the name and location of a valid script.

Dest_IP_Address (0x456001f)

Specifies the destination IP address. This parameter is used for DNS, ICMP, Jitter, SMTP, TCP, Trace Route, and UDP tests.

Dest_Password (0x456000e)

Important! The Dest_Password parameter is used for FTP, HTTP, HTTPS, POP3, SMTP, and SQL Query tests. You cannot use the CLI or the REST API for this parameter, as this password value is encrypted in the CA Spectrum database. Use the OneClick console to enter this value.

Dest_Port_Number (0x4560011)

Specifies the port number where the service is running for FTP, Jitter, POP3, SMTP, TCP, and UDP tests. For Mean Opinion Score (MOS) support in Jitter tests, the destination port must be an even-numbered port in the range 16384 - 32766 or 49152 - 65534.

Note: Dest_Port_Number is supported for FTP, POP3, and SMTP tests only for SystemEDGE hosts.

Dest_URL (0x456000f)

Specifies the destination URL required for HTTP tests. Enclose the URL between double quotes (“ ”), and use escape slashes (\) before forward slashes (/). See Create Tests in CLI (see page 80) for a format example.

Dest_User_Name (0x456000b)

Specifies the destination user name, which is required for FTP and POP3 tests and optional for HTTP and HTTPS tests. For SMTP tests, this required parameter is the email address that you want to test. For SQL Query tests, this required parameter is the username for database access.

Query_String (0x456010c)

Specifies the query statement to execute. This parameter is required for SQL Query tests.

SQL_Driver (0x4560109)

Specifies the name of the SQL driver, which is required for some SQL Query tests, depending on the database type.

Example:

```
com.mysql.jcbc.Driver
```

Optional Parameters

You can use optional parameters to specify various optional test parameters.

Note: Configure Advanced Parameters (see page 45) describes how to specify these parameters using the Service Performance Manager user interface in OneClick.

CodecType (0x45600e7)

Specifies the type of codec that is used by the router to perform audio compression and decompression. This parameter is important for calculating the Mean Option Score (MOS).

0 = None

1 = G.711 U-law

2 = G.711 A-law

3 = G.729A

Default: 0

DeleteMessages (0x45600f5)

Specifies whether to delete the messages that were downloaded during the test or to leave the messages on the test system.

Default: False

Note: DeleteMessages is supported for POP3 tests for SystemEDGE hosts only.

DownloadContent (0x45600fd)

Specifies whether to download all images, frames, scripts, and applets, with the core HTML code from the website or URL.

Default: False

Note: DownloadContent is supported for HTTP and HTTPS tests for SystemEDGE hosts only.

DownloadType (0x45600f4)

Specifies whether the first or all messages are downloaded for POP3 tests.

1 = Download only the first message for this user account.

2 = Download all messages for this user account.

Default: 1

Note: DownloadType is supported for POP3 tests for SystemEDGE hosts only.

EchoAdminSourceAddress (0x45600b0)

Specifies the IP address or hostname of the test when it is not the test host. For more information, see About the Test Host Location Parameter (see page 43).

Note: EchoAdminSourceAddress is supported for Cisco hosts only.

EchoAdminSourcePort (0x45600b1)

Specifies the port number that is used by the tested application (Jitter, TCP, UDP only).

Limits: Must be less than 65536

Note: EchoAdminSourcePort is supported for Cisco hosts only.

FailOnContentError (0x45600fe)

Specifies whether any errors that are encountered while downloading images, frames, scripts, and applets cause the test to fail.

Default: False

Note: FailOnContentError is supported for HTTP and HTTPS tests for SystemEDGE hosts only.

FILTER_TIMEOUT_DATA (0x45600d6)

Specifies whether the RTM_Test generates result events for timeouts.

Default: True

FrameDepth (0x45600fa)

Specifies the number of levels the test should traverse when downloading nested frames. The HTTP and HTTPS tests download all frames, images, external scripts, and applets during the page download. The measurement reflects your experience when downloading a web page.

Default: 3

Note: FrameDepth is supported for HTTP and HTTPS for SystemEDGE hosts only.

MailBodySize (0x45600f6)

Specifies the size (in bytes) of the test message to send.

Default: 1000

Note: MailBodySize is supported for SMTP tests for SystemEDGE hosts only.

MinMatches (0x45600fc)

Specifies the minimum number of times that the search expression can be found. The test fails if the search expression is not found for the specified number of times.

Default: 1

Note: MinMatches is supported for HTTP and HTTPS tests for SystemEDGE hosts only.

OperationType (0x45600f3)

Specifies the type of FTP operation to test.

1 = Login

2 = Get

3 = Put

Default: 1

Note: OperationType is supported for FTP tests for SystemEDGE hosts only.

OtherUserName (0x45600f8)

Specifies a username. For SMTP tests for SystemEDGE hosts, this is the outgoing username for SMTP authentication. For HTTP tests for Cisco routers and HTTP and HTTPS tests for SystemEDGE hosts, it is a valid username to be authenticated on the specified proxy server.

OtherPassword (0x45600f9)

Important! The OtherPassword parameter is used for the Outgoing Password value for SMTP tests for SystemEDGE hosts. It is also used for the Proxy Password value for HTTP and HTTPS tests for Cisco routers and SystemEDGE hosts. Because this password value is encrypted in the CA Spectrum database, you cannot use CLI for this parameter. Use the OneClick Console to enter this value.

Packet_Size (0x4560067)

Specifies the value (expressed in octets) that limits the size of the packets that are used in the test.

Default: 64

Proxy_URL (0x456008d)

Specifies a proxy URL or server.

For Proxy URL, enclose the URL between double quotes (“ ”), and use escape slashes (\ ) before forward slashes (/). See Create Tests in CLI (see page 80) for a format example using a URL.

For Proxy Server (for SystemEDGE hosts only), use the format <*server*>[:*port*].

Note: Proxy_URL is supported for HTTP and HTTPS tests only.

Sample_Count (0x4560068)

Specifies the number of times during a test run that the test is performed.

Default: 5

Source_IP_Address (0x45600f2)

Specifies the source IP address.

Note: Source_IP_Address is supported for Mid_Path/Extended_Path Ping tests only.

State (0x4560003)

Specifies the test state:

1 = Enabled

2 = Disabled

Default: 1

Test_Host_Position (0x4560030)

Specifies test host location.

0 = End point

1 = Mid path

2 = Extended path

Default: 0

TextMatch (0x45600fb)

Specifies a regular expression or text string to match on the pages you test.

Note: TextMatch is supported for HTTP and HTTPS tests for SystemEDGE hosts only.

Thresh_Model (0x4560024)

Specifies the test entity where threshold events are asserted.

0 = Test

1 = Source

2 = Destination

3 = Host

Default: 0

THRESH_SCHED_MH (0x4560090)

Specifies the Model Handle of a Schedule model. This parameter is used with the ThreshSchedule_Type parameter. Not specifying a value results in a 7x24 schedule.

ThreshSchedule_Type (0x4560090)

Specifies preconfigured threshold schedules for periods during which you want to see Service Performance Manager threshold alarms. Not specifying a value results in a 7x24 schedule.

0 = 7x24

1 = 7A-6P

2 = 6P-7A

3 = MF 8A-8P

4 = MF 6A-11P

Default: 0

TypeOfService (0x4560099)

Specifies the Type of Service (TOS) octet in an IP datagram header that enables packets with different TOS values to be routed differently.

Limits: Must be less than 256

Default: 0

UseSSL (0x45600f7)

Specifies whether to enable Secure Sockets Layer security in case the SMTP server requires SSL authentication.

Default: False

Note: UseSSL is supported for SMTP tests for SystemEDGE hosts only.

Required Parameters for Scheduling Tests

Use these parameters to specify test timeout and test schedule management values.

Note: Schedule a Test (see page 49) explains the procedure to configure test schedule parameters using the Service Performance Manager user interface in OneClick.

ACTIVE_SCHED_MH (0x456008f)

Specifies the model handle of a test schedule model. Use this parameter as an alternative to TestSchedule_Type. Not specifying a value results in a 7x24 schedule.

Schedule_State (0x4560000)

Specifies whether the test schedule is in effect.

0 = Disables

1 = Enabled

Default: 0

Sched_Frequency (0x4560014)

Specifies the interval in seconds between scheduled test runs.

Default: 5000

Test_Timeout (0x4560025)

Specifies the number of milliseconds before a test connection to an unresponsive test host times out.

Default: 5000

TestSchedule_Type (0x456008b)

Specifies preconfigured test schedules. Use this parameter as an alternative to ACTIVE_SCHED_MH. Not specifying a value results in a 7x24 schedule.

0 = 7x24

1 = 7A-6P

2 = 6P-7A

3 = MF 8A-8P

4 = MF 6A-11P

Default: 5

Thresh_Frequency (0x456001a)

Specifies an interval in seconds after which a test runs while in a threshold condition.

Default: 300

Threshold Type Parameters

You can specify threshold management parameters for all test types. Thresholds are expressed either in terms of response, or transaction time, or packet error or loss, depending on the type of test for which the threshold is specified.

Latency Threshold Parameters

Latency_Thresh_State (0x4560035)

Specifies whether the latency threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

Latency_MinorSetValue (0x456009b)

Specifies the latency threshold period in milliseconds that must be exceeded before a minor alarm is generated.

Default: 500

Latency_MajorSetValue (0x456009c)

Specifies the latency threshold period in milliseconds that must be exceeded before a major alarm is generated.

Default: None

Latency_CriticalSetValue (0x456009d)

Specifies the latency threshold period in milliseconds that must be exceeded before a critical alarm is generated.

Default: None

Thresh_Set_Value (0x4560016)

Specifies the latency threshold period in milliseconds that must be exceeded before an event is generated.

Default: None

Thresh_Clear_Value (0x4560017)

Specifies the latency threshold period in milliseconds the test must not exceed before an event is cleared.

Default: 500

Thresh_Set_Delay (0x4560026)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 1

Thresh_Clear_Delay (0x4560027)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

Packet Loss Threshold Parameters

PL_Thresh_State (0x4560034)

Specifies whether the packet loss threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

PacketLoss_MinorSetValue (0x456009e)

Specifies the packet lost percentage that must be exceeded before a minor alarm is generated.

Default: 20percent

PacketLoss_MajorSetValue (0x456009f)

Specifies the packet lost percentage that must be exceeded before a major alarm is generated.

Default: None

PacketLoss_CriticalSetValue (0x45600a0)

Specifies the packet lost percentage that must be exceeded before a critical alarm is generated.

Default: None

PL_Set_Value (0x456002c)

Specifies the packet lost percentage that must be exceeded before an event is generated.

Default: None

PL_Clear_Value (0x456002e)

Specifies the packet lost percentage that must not be exceeded before a minor alarm is generated.

Default: 20percent

PL_Set_Delay (0x456002d)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 1

PL_Clear_Delay (0x456002f)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

HTTP DNS Threshold Parameters

Statistic_1_Thresh_State (0x4560036)

Specifies whether the HTTP DNS threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

Statistic_1_MinorSetValue (0x45600a1)

Specifies the resolution time threshold period in milliseconds that must be exceeded before a minor alarm is generated.

Default: 500

Statistic_1_MajorSetValue (0x45600a2)

Specifies the resolution time threshold period in milliseconds that must be exceeded before a major alarm is generated.

Default: None

Statistic_1_CriticalSetValue (0x45600a3)

Specifies the resolution time threshold period in milliseconds that must be exceeded before a critical alarm is generated.

Default: None

Statistic_1_Set_Value (0x4560039)

Specifies the resolution time threshold period in milliseconds that must be exceeded before an event is generated.

Default: None

Statistic_1_Clear_Value (0x456003a)

Specifies the resolution time threshold the test must not exceed before an event is cleared.

Default: 500

Statistic_1_Set_Delay (0x456003b)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 1

Statistic_1_Clear_Delay (0x456003c)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

HTTP TCP Threshold Parameters

Statistic_2_Thresh_State (0x456003e)

Specifies whether the HTTP TCP threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

Statistic_2_MinorSetValue (0x45600a4)

Specifies the connection time threshold period in milliseconds that must be exceeded before a minor alarm is generated.

Default: 500

Statistic_2_MajorSetValue (0x45600a5)

Specifies the connection time threshold period in milliseconds that must be exceeded before a major alarm is generated.

Default: None

Statistic_2_CriticalSetValue (0x45600a6)

Specifies the connection time threshold period in milliseconds that must be exceeded before a critical alarm is generated.

Default: None

Statistic_2_Set_Value (0x4560041)

Specifies the connection time threshold period in milliseconds that must be exceeded before an event is generated.

Default: None

Statistic_2_Clear_Value (0x4560042)

Specifies the connection time threshold that must not exceed before an event is cleared.

Default: 500

Statistic_2_Set_Delay (0x4560043)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 1

Statistic_2_Clear_Delay (0x4560044)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

HTTP Download Threshold Parameters

Statistic_3_Thresh_State (0x4560046)

Specifies whether the HTTP download threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: None

Statistic_3_MinorSetValue (0x45600a7)

Specifies the download time threshold period in milliseconds that must be exceeded before a minor alarm is generated.

Default: 500

Statistic_3_MajorSetValue (0x45600a8)

Specifies the download time threshold period in milliseconds that must be exceeded before a major alarm is generated.

Default: None

Statistic_3_CriticalSetValue (0x45600a9)

Specifies the download time threshold period in milliseconds that must be exceeded before a critical alarm is generated.

Default: None

Statistic_3_Set_Value (0x4560049)

Specifies the download time threshold period in milliseconds that must be exceeded before an event is generated.

Default: None

Statistic_3_Clear_Value (0x456004a)

Specifies the download time latency threshold the test must not exceed before an event is cleared.

Default: 500

Statistic_3_Set_Delay (0x456004b)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 1

Statistic_3_Clear_Delay (0x456004c)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

Jitter Source to Destination Packet Loss Threshold

Statistic_1_Thresh_State (0x4560036)

Specifies whether the Jitter source to destination packet loss threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

Statistic_1_MinorSetValue (0x45600a1)

Specifies the percentage of packets that must be lost before a minor alarm is generated.

Default: 20percent

Statistic_1_MajorSetValue (0x45600a2)

Specifies the percentage of packets that must be lost before a major alarm is generated.

Default: None

Statistic_1_CriticalSetValue (0x45600a3)

Specifies the percentage of packets that must be lost before a critical alarm is generated.

Default: None

Statistic_1_Set_Value (0x4560039)

Specifies the percentage of packets that must be lost before an event is generated.

Default: None

Statistic_1_Clear_Value (0x456003a)

Specifies the percentage of packets lost that cannot be exceeded before an event or alarm is cleared.

Default: 20percent

Statistic_1_Set_Delay (0x456003b)

Specifies the number of consecutive cycles the test must run in violation of a threshold before an event or alarm is generated.

Default: 1

Statistic_1_Clear_Delay (0x456003c)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

Jitter Destination to Source Packet Loss Threshold

Statistic_2_Thresh_State (0x456003e)

Specifies whether the Jitter destination to source packet loss threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

Statistic_2_MinorSetValue (0x45600a4)

Specifies the packet lost percentage that must be exceeded before a minor alarm is generated.

Default: 20percent

Statistic_2_MajorSetValue (0x45600a5)

Specifies the packet lost percentage that must be exceeded before a major alarm is generated.

Default: None

Statistic_2_CriticalSetValue (0x45600a6)

Specifies the packet lost percentage that must be exceeded before a critical alarm is generated.

Default: None

Statistic_2_Set_Value (0x4560041)

Specifies the packet lost percentage that must be exceeded before an event is generated.

Default: None

Statistic_2_Clear_Value (0x4560042)

Specifies the packet lost percentage that must not be exceeded before a minor alarm is generated.

Default: 20percent

Statistic_2_Set_Delay (0x4560043)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 1

Statistic_2_Clear_Delay (0x4560044)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

Jitter MIA Threshold Parameters

Statistic_3_Thresh_State (0x4560046)

Specifies whether the Jitter MIA threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

Statistic_3_MinorSetValue (0x45600a7)

Specifies the percentage of missing in action packets that must be exceeded before a minor alarm is generated.

Default: 20percent

Statistic_3_MajorSetValue (0x45600a8)

Specifies the percentage of missing in action packets that must be exceeded before a major alarm is generated.

Default: None

Statistic_3_CriticalSetValue (0x45600a9)

Specifies the percentage of missing in action packets that must be exceeded before a critical alarm is generated.

Default: None

Statistic_3_Set_Value (0x4560049)

Specifies the percentage of missing in action packets that must be exceeded before an event is generated.

Default: None

Statistic_3_Clear_Value (0x456004a)

Specifies the percentage of missing in action packets that must not be exceeded before an event or alarm is cleared.

Default: 20percent

Statistic_3_Set_Delay (0x456004b)

Specifies the number of consecutive cycles the test must exceed the threshold before an event or alarm is generated.

Default: 1

Statistic_3_Clear_Delay (0x456004c)

Specifies the number of consecutive cycles the test must not exceed the threshold before an event or alarm is generated.

Default: 1

Jitter Late Arrival Threshold Parameters

Statistic_4_Thresh_State (0x456004e)

Specifies whether the Jitter late arrival threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

Statistic_4_MinorSetValue (0x45600aa)

Specifies the percentage of late packets that must be exceeded before a minor alarm is generated.

Default: None

Statistic_4_MajorSetValue (0x45600ab)

Specifies the percentage of late packets that must be exceeded before a major alarm is generated.

Default: 20percent

Statistic_4_CriticalSetValue (0x45600ac)

Specifies the percentage of late packets that must be exceeded before a critical alarm is generated.

Default: None

Statistic_4_Set_Value (0x4560051)

Specifies the percentage of late packets that must be exceeded before an event is generated.

Default: None

Statistic_4_Clear_Value (0x4560052)

Specifies the percentage of late packets that must not be exceeded before an event or alarm is cleared.

Default: None

Statistic_4_Set_Delay (0x4560053)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 20percent

Statistic_4_Clear_Delay (0x4560054)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

Jitter Busies Threshold Parameters

Statistic_5_Thresh_State (0x4560056)

Specifies whether the Jitter busies threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

Statistic_5_MinorSetValue (0x45600ad)

Specifies the percentage of busy failures that must be exceeded before a minor alarm is generated.

Default: 20

Statistic_5_MajorSetValue (0x45600ae)

Specifies the percentage of busy failures that must be exceeded before a major alarm is generated.

Default: None

Statistic_5_CriticalSetValue (0x45600af)

Specifies the percentage of busy failures that must be exceeded before a critical alarm is generated.

Default: None

Statistic_5_Set_Value (0x4560059)

Specifies the percentage of busy failures that must be exceeded before an event is generated.

Default: None

Statistic_5_Clear_Value (0x456005a)

Specifies the percentage of busy failures that must not be exceeded before an event is generated.

Default: 20

Statistic_5_Set_Delay (0x456005b)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 1

Statistic_5_Clear_Delay (0x456005c)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

Jitter Positive Source to Destination Threshold Parameters

Statistic_6_Thresh_State (0x45600ba)

Specifies whether the Jitter positive source to destination threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

Statistic_6_MinorSetValue (0x45600b4)

Specifies the percentage of positive Jitter that must be exceeded before a minor alarm is generated.

Default: 25

Statistic_6_MajorSetValue (0x45600b5)

Specifies the percentage of positive Jitter that must be exceeded before a major alarm is generated.

Default: None

Statistic_6_CriticalSetValue (0x45600b6)

Specifies the percentage of positive Jitter that must be exceeded before a critical alarm is generated.

Default: None

Statistic_6_Set_Value (0x45600b3)

Specifies the percentage of positive Jitter that must be exceeded before an event is generated.

Default: None

Statistic_6_Clear_Value (0x45600b7)

Specifies the percentage of positive Jitter that must not be exceeded before an event is generated.

Default: 25

Statistic_6_Set_Delay (0x45600b8)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 1

Statistic_6_Clear_Delay (0x45600b9)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

Jitter Positive Destination to Source Threshold Parameters

Statistic_7_Thresh_State (0x45600ce)

Specifies whether the Jitter positive destination to source threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

Statistic_7_MinorSetValue (0x45600bd)

Specifies the percentage of positive Jitter that must be exceeded before a minor alarm is generated.

Default: 25

Statistic_7_MajorSetValue (0x45600be)

Specifies the percentage of positive Jitter that must be exceeded before a major alarm is generated.

Default: None

Statistic_7_CriticalSetValue (0x45600bf)

Specifies the percentage of positive Jitter that must be exceeded before a critical alarm is generated.

Default: None

Statistic_7_Set_Value (0x45600bc)

Specifies the percentage of positive Jitter that must be exceeded before an event is generated.

Default: None

Statistic_7_Clear_Value (0x45600c0)

Specifies the percentage of positive Jitter that must not be exceeded before an event is generated.

Default: 25

Statistic_7_Set_Delay (0x45600c1)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 1

Statistic_7_Clear_Delay (0x45600c2)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 25

Jitter Negative Source to Destination Threshold Parameters

Statistic_8_Thresh_State (0x45600cc)

Specifies whether the Jitter negative source to destination threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

Statistic_8_MinorSetValue (0x45600c5)

Specifies the percentage of negative Jitter that must be exceeded before a minor alarm is generated.

Default: 25

Statistic_8_MajorSetValue (0x45600c6)

Specifies the percentage of negative Jitter that must be exceeded before a major alarm is generated.

Default: None

Statistic_8_CriticalSetValue (0x45600c7)

Specifies the percentage of negative Jitter that must be exceeded before a critical alarm is generated.

Default: None

Statistic_8_Set_Value (0x45600c5)

Specifies the percentage of negative Jitter that must be exceeded before an event is generated.

Default: None

Statistic_8_Clear_Value (0x45600c9)

Specifies the percentage of negative Jitter that must not be exceeded before an event is generated.

Default: 25

Statistic_8_Set_Delay (0x45600ca)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 1

Statistic_8_Clear_Delay (0x45600cb)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

Jitter Negative Destination to Source Threshold Parameters

Statistic_9_Thresh_State (0x45600d5)

Specifies whether the Jitter negative destination to source threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: None

Statistic_9_MinorSetValue (0x45600cf)

Specifies the percentage of negative Jitter that must be exceeded before a minor alarm is generated.

Default: 25

Statistic_9_MajorSetValue (0x45600d0)

Specifies the percentage of negative Jitter that must be exceeded before a major alarm is generated.

Default: None

Statistic_9_CriticalSetValue (0x45600d1)

Specifies the percentage of negative Jitter that must be exceeded before a critical alarm is generated.

Default: None

Statistic_9_Set_Value (0x45600ce)

Specifies the percentage of negative Jitter that must be exceeded before an event is generated.

Default: None

Statistic_9_Clear_Value (0x45600d2)

Specifies the percentage of negative Jitter that must not be exceeded before an event is generated.

Default: 25

Statistic_9_Set_Delay (0x45600d3)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 1

Statistic_9_Clear_Delay (0x45600d4)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

Packet out of Sequence SD Threshold Parameters

POOS_SD_ThreshState (0x4560119)

Specifies whether the Packets out of Sequence SD threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

POOS_SD_MinorSetValue (0x4560113)

Specifies the percentage of Packets out of Sequence SD that must be exceeded before a minor alarm is generated.

Default: 25

POOS_SD_MajorSetValue (0x4560114)

Specifies the percentage of Packets out of Sequence SD that must be exceeded before a major alarm is generated.

Default: None

POOS_SD_CriticalSetValue (0x4560115)

Specifies the percentage of Packets out of Sequence SD that must be exceeded before a critical alarm is generated.

Default: None

POOS_SD_SetValue (0x4560112)

Specifies the percentage of Packets out of Sequence SD that must be exceeded before an event is generated.

Default: None

POOS_SD_ClearValue (0x4560116)

Specifies the percentage of Packets out of Sequence SD that must not be exceeded before an event or alarm is cleared.

Default: 25

POOS_SD_SetDelay (0x4560117)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 1

POOS_SD_ClearDelay (0x4560118)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

Packet out of Sequence DS Threshold Parameters

POOS_DS_ThreshState (0x4560124)

Specifies whether the Packets out of Sequence DS threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

POOS_DS_MinorSetValue (0x456011e)

Specifies the percentage of Packets out of Sequence DS that must be exceeded before a minor alarm is generated.

Default: 25

POOS_DS_MajorSetValue (0x456011f)

Specifies the percentage of Packets out of Sequence DS that must be exceeded before a major alarm is generated.

Default: None

POOS_DS_CriticalSetValue (0x4560120)

Specifies the percentage of Packets out of Sequence DS that must be exceeded before a critical alarm is generated.

Default: None

POOS_DS_SetValue (0x456011d)

Specifies the percentage of Packets out of Sequence DS that must be exceeded before an event is generated.

Default: None

POOS_DS_ClearValue (0x4560121)

Specifies the percentage of Packets out of Sequence DS that must not be exceeded before an event or alarm is cleared.

Default: 25

POOS_DS_SetDelay (0x4560122)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 1

POOS_DS_ClearDelay (0x4560123)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

Packet out of Sequence BOTH Threshold Parameters

POOS_BOTH_ThreshState (0x456012f)

Specifies whether the Packets out of Sequence BOTH threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

POOS_BOTH_MinorSetValue (0x4560129)

Specifies the percentage of Packets out of Sequence BOTH that must be exceeded before a minor alarm is generated.

Default: 25

POOS_BOTH_MajorSetValue (0x456012a)

Specifies the percentage of Packets out of Sequence BOTH that must be exceeded before a major alarm is generated.

Default: None

POOS_BOTH_CriticalSetValue (0x456012b)

Specifies the percentage of Packets out of Sequence BOTH that must be exceeded before a critical alarm is generated.

Default: None

POOS_BOTH_SetValue (0x4560128)

Specifies the percentage of Packets out of Sequence BOTH that must be exceeded before an event is generated.

Default: None

POOS_BOTH_ClearValue (0x456012c)

Specifies the percentage of Packets out of Sequence BOTH that must not be exceeded before an event or alarm is cleared.

Default: 25

POOS_BOTH_SetDelay (0x456012d)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 1

POOS_BOTH_ClearDelay (0x456012e)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

Packet Skipped Threshold Parameters

PSKIPPED_ThreshState (0x456013a)

Specifies whether the Packets Skipped threshold is enabled or disabled for a test.

0 = Disabled

1 = Enabled

Default: 0

PSKIPPED_MinorSetValue (0x4560134)

Specifies the percentage of Packets Skipped that must be exceeded before a minor alarm is generated.

Default: 25

PSKIPPED_MajorSetValue (0x4560135)

Specifies the percentage of Packets Skipped that must be exceeded before a major alarm is generated.

Default: None

PSKIPPED_CriticalSetValue (0x4560136)

Specifies the percentage of Packets Skipped that must be exceeded before a critical alarm is generated.

Default: None

PSKIPPED_SetValue (0x4560133)

Specifies the percentage of Packets Skipped that must be exceeded before an event is generated.

Default: None

PSKIPPED_ClearValue (0x4560137)

Specifies the percentage of Packets Skipped that must not be exceeded before an event or alarm is cleared.

Default: 25

PSKIPPED_SetDelay (0x4560138)

Specifies the number of consecutive cycles the test must run in violation of the threshold before an event or alarm is generated.

Default: 1

PSKIPPED_ClearDelay (0x4560139)

Specifies the number of consecutive cycles the test must run without exceeding the threshold before an event or alarm is cleared.

Default: 1

Test Action Codes

Use action codes with the CLI update command to discover tests, save changes to tests, run tests, and control timeout debugging information.

Discover tests (0x4560007)

Specifies to run SPM Test Discovery to discover and model performance tests that are configured on test hosts and not with Service Performance Manager. Use this action code with the RTM_TestHost model.

Update test (0x4560008)

Specifies to update test after making attribute changes.

Run test (0x4560009)

Specifies to run the test.

Update and Run test (0x456000a)

Specifies to run a combination of the Update and Run actions.

Include Timeout Debugging Information (0x456000e)

Specifies to include diagnostic information with SPM Timeout Event description.

Turn Off Timeout Debugging Information (0x456000f)

Specifies not to include diagnostic information with SPM Timeout Event description.

Test Status and Test Results Parameters

SPM LatestStatus (0x4560004) Attribute Values

You can use the latest status attribute with the CLI show command to get status information for the most recently run test.

1 = Ok

Test ran successfully.

2 = Threshold

Test result has exceeded its Set Value.

3 = Timeout

Test timed out.

4 = Failed

Test failed to create a response time test table entry due to configuration issue.

5 = Initial

Test has never run.

6 = Bad_comm

Test failed to create a response time test table entry because of an invalid community string.

7 = Running

Test is running.

8 = Stopped

Test has stopped running.

9 = Threshold_minor

Test result has exceeded its Minor Set Value.

10 = Threshold_major

Test result has exceeded its Major Value.

11 = Threshold_critical

Test result has exceeded its Critical Value.

Test Results

Use the CLI show command to get results for a particular test.

Result_Timestamp (0x456005e)

The time test last completed.

Latest_Result (0x4560015)

Average Response Time (scalar).

TRACEROUTE_Result (0x4560075)

TraceRoute Result. List of IP Address Latency Result pairs.

PL_Result (0x456007d)

% Packet Loss.

DNS_Latest_Result (0x4560037)

Average HTTP DNS Lookup Time (scalar).

TCP_Latest_Result (0x456003f)

Average HTTP TCP Connection Time (scalar).

DL_Latest_Result (0x4560047)

Average HTTP Page Download Time (scalar).

JPLSD_Latest_Result (0x456007e)

% Jitter Packets Loss between Source and Destination.

JPLDS_Latest_Result (0x456007f)

% Jitter Packets Loss between Destination and Source.

JBUS_Latest_Result (0x4560080)

% Jitter Packets Busy.

JMIA_Latest_Result (0x4560081)

% Jitter Packets Missing in Action.

JLATE_Latest_Result (0x4560082)

% Jitter Packets Arriving Late.

PosJitterSD_LatestResult (0x45600b2)

Average Positive Jitter between Source and Destination.

PosJitterDS_LatestResult (0x45600bb)

Average Positive Jitter between Destination and Source.

NegJitterSD_LatestResult (0x45600c4)

Average Negative Jitter between Source and Destination.

NegJitterDS_LatestResult (0x45600cd)

Average Negative Jitter between Destination and Source.

MOS_Latest_Result (0x45600e5)

Mean Opinion Score Value (0 - 500). It provides a numerical measure of the quality of human speech at the destination end of the circuit.

Appendix A: Troubleshooting

This chapter identifies error messages that may be generated during Service Performance Manager operations and describes corrective action where feasible. Other maintenance and optional configuration issues are also addressed.

This section contains the following topics:

Firmware Issues

Certain router firmware revisions can exhibit instability. CA follows published interfaces to the SNMP agents, and rely on the device vendors to fully support these interfaces. Before deploying Service Performance Manager, it is advisable that users review device and firmware documentation from the vendor and apply any updates as appropriate.

Cisco IOS

When managing Jitter tests on Cisco IP SLA hosts, certain Cisco IOS versions do not allow codec type changes once the test has been run.

Cisco IOS 12.0(9)

Cisco IOS 12.0(9) has an issue that causes the router to reload upon the first SNMP SET performed to validate that the MIB is writable. For more information, see http://www.cisco.com/en/US/docs/ios/12_0/release/notes/120mcavs.html.

Cisco IOS 12.0(9) has an issue that causes the router to reload upon an SNMP Get of the supported test types table, which occurs during model activation.

Cisco IOS 12.0(7)T2

Cisco IOS 12.0(7)T2 has an issue which causes the test that is described in Traceroute Tests (see page 31) to fail. The problem is that the device does not report hop data correctly in the result tables of the CISCO-RTTMON-MIB, which causes Service Performance Manager to put erroneous data in the result event for average response time. To address this issue, upgrade your firmware to Cisco IOS 12.1(17).

Cisco IOS below 12.2

Cisco IOS below 12.2 has an issue which causes HTTP version 1.1 tests to fail with a “Request Timed Out” error message. Upgrading to Cisco IOS 12.2 or later versions will fix this issue.

Workaround: Changing the HTTP version from 1.1 to 1.0 may correct the timeout error message. See Configure Advanced Parameters (see page 45) for more information.

Cisco IOS 12.2(2)T

Cisco IOS 12.2(2)T has an issue that causes the router to intermittently report incorrect operation error codes such as DHCP response time tests that have timed out are reported as OK. If you encounter this issue during a run of a DHCP test, Service Performance Manager can report a latency value for the DHCP test, greater than the timeout value set for the test. To address this issue, Cisco recommends upgrading your firmware to Cisco IOS 12.2(15)T2.

Cisco IOS 12.2(11)T

Cisco devices running IOS firmware 12.2(11)T and higher correctly function as test hosts in Service Performance Manager. Previously, configured tests would not operate correctly due to changes in the RTTMon MIB.

Cisco IOS 12.3(4)

When running Service Performance Manager tests, a router running Cisco IOS version 12.3(10a) that is configured for SAA/RTR may crash because of a memory leak in the SAA/RTR process. This issue has been resolved in IOS version 12.3 (11) TO4.

Cisco IOS 12.3(5) and below

In Cisco IOS 12.3(5) and lower versions, changing the packet size on a Jitter Tests (see page 30) can cause the IOS to crash and reboot the router. This issue is addressed in Cisco IOS 12.3(5.013).

Cisco IOS 12.2(18)SXF3 and 12.2(18)SXF4

Cisco Routers running IOS 12.2(18)SXF3 with version 12.2(18)SXF4 can crash, when Service Performance Manager tests are run. Because of Cisco bug CSCin62031, the router can crash. Routers running these IOS versions cannot be modeled as test hosts capable of running Cisco IPSLA. To prevent these routers from being modeled as test hosts capable of running Cisco IPSLA, add the following commands to the router configuration before modeling:

```
snmp-server view NoRTTMON internet included

snmp-server view NoRTTMON ciscoRttMonMIB excluded

snmp-server community TEST view NoRTTMON RO
```

If these configuration commands are added after modeling, any attempt to run Service Performance Manager tests fails and do not let the router to crash.

Juniper (all JUNOS devices)

On a Juniper host device, running a response time test with a name longer than 32 characters returns an error. If you see such an error, recreate the test with a shorter name. When test templates are used, be aware that the model name or IP address is appended onto the template name. Be sure to leave enough characters when using templates so that the final, full test name reaches or falls below the 32 character limit.

Riverstone RS-8000 FW 9.0.0.4

Response time tests that are run from Riverstone RS-8000 (firmware 9.0.0.4) test host devices can return Bad Configuration errors. If you see these errors, verify that no two tests (configured for the Riverstone test host) have names with the same character length. If necessary, rename any such tests. For more information, see Configure General Parameters (see page 40).

Timeout Errors

In most cases, lack of access is the cause of timeout errors during Service Performance Manager tests. For example, when Network Address Translation (NAT) is enabled, it can deny access to networks that are not in the list of networks to translate. Thus response time tests for HTTP or ICMP echo from an unlisted range of IPs would result in timeouts.

The solution in this case is to add the test network to the NAT list and rerun the tests. Other tests, such as DNS, DHCP, and UDP require the test host device to be properly configured for the service to be tested.

Timeout errors can also be caused by setting the latency timeout parameter to an invalid value. Valid values for test timeouts can vary from one test type to another, and from one device to another. For example, the CISCO-RTTMON-MIB provides the following guideline in describing its timeout value:

```
To prevent unwanted closure of connections, be sure to set this value to a realistic
connection timeout.
```

You can verify the following common solutions for timeout errors:

- Verify that you have SNMP read/write access on the test host device.
- Verify that you have access from the test host device to the service being tested (such as ICMP, HTTP).
- Verify that you have set reasonable values for a test timeout.

Note: HTTP tests using certain Cisco Routers that run HTTP version 1.1 can fail with a Request Timed Out error. For more information, see Firmware Issues (see page 113).

ICMP Ping Tests and Extreme Summit Test Host Devices

Ping tests that are run from Extreme Summit test host devices can result in timeouts. When you execute a ping from certain Extreme Summit devices, the RFC2925 branch of their MIB agents incorrectly reports a response time of 0. Service Performance Manager interprets this issue as a timeout, when in fact the device has replied to the ping. The current workaround is to use a different device as a test host.

Traceroute Tests and iAgent Test Hosts

Service Performance Manager always reports a timeout when traceroute tests are run on an iAgent test host. This issue is resolved by iAgent version 16.2.

Add Debugging Information to a Timeout Event

When attempting to determine the cause of a timeout event, you can collect diagnostic information for use by CA Support. Use the Command Line Interface to send an action to a test model so that it includes debugging information with the timeout event.

Using a CLI command, you can add debugging information to a timeout event and also disable debugging.

Follow these steps:

1. Open the Command Line Interface and enter the following command:

   ```
   update action=0x456000e mh=<RTM_Test Model_Handle>
   ```

   where *RTM_Test Model_Handle* is the Model_Handle attribute for the test model.

2. Add the following information to the SPM Timeout Event description:

   ```
   Additional Info: id xxxxx error: yy
   ```

   The information is added to the SPM Timeout Event description.

3. To disable debugging, use the following command:

   ```
   update action=0x456000f mh=<RTM_Test Model_Handle>
   ```

   where *RTM_Test Model_Handle* is the Model_Handle attribute for the test model.

   Debugging is disabled.

Note: For more information, see the *Command Line Interface User Guide*.

Scheduling Tests in Geographically Distributed Environments

In a geographically distributed environment, the following network components can potentially be in different time zones:

- SpectroSERVERs
- OneClick consoles
- Web servers
- Test host devices

Test scheduling in Service Performance Manager is based on the time zone of the SpectroSERVER where the test host is modeled. Test results are based on the time zone of the OneClick console. To address the time discrepancy, select the 24/7 option when scheduling.

SpectroSERVER Crashed while Deleting the RTM_Hosts

Symptom:

When RTM_Hosts are deleted from Service Performance Manager, SpectroSERVER crashes.

Solution:

RTM Test Hosts are automatically created when a device is modeled and it supports the RTTMON application You must not delete these models. These models lets you know the device that supports the RTTMON application.

Delayed SpectroSERVER Activation Resulting from External Reads

For agents that support performance test types through MIB objects, CA Spectrum must perform external reads of these MIB objects at SpectroSERVER activation time to obtain the list of supported test types. This action can delay the SpectroSERVER activation time. You can configure the spm_wait_activate parameter in the .vnmrc file to delay the external reads until the SpectroSERVER is activated.

Set the default value of spm_wait_activate from No to Yes to prevent Service Performance Manager from performing external reads until the SpectroSERVER is activated.

Note: The agent test host remains inactive until the SpectroSERVER is activated.

Appendix B: Event Codes

This section contains the following topics:

About SPM Timeout Event

Service Performance Manager determines when it is appropriate to generate an SPM Timeout Event and its associated alarm:

- SPM Timeout Event and its related alarm are suppressed, if the destination IP of the test represents a CA Spectrum device model that does not have ICMP contact. The alarm appears as a symptom of the DEVICE HAS STOPPED RESPONDING TO POLLS alarm of the CA Spectrum device model.
- SPM Timeout Event and its related alarm are not generated, if the test host does not have SNMP contact at the time that the RTM results are read for a given Service Performance Manager test.

Event Code Descriptions

The following table lists Service Performance Manager events by event code, event name, the model types that event can be asserted on, the alarm that is generated or cleared (if any), and the alarm severity.

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x04560000	SPM Result Event	RTM_Test	None	N/A
0x04560001	SPM Timeout Event. For more information, see About SPM Timeout Event (see page 119).	RTM_Test	0x04560001	Yellow
0x04560002	SPM Test Host Configuration Failed Event	RTM_Test	0x04560002	Yellow

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x04560003	SPM Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x04560004	SPM Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560003	Yellow
0x04560005	SPM Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560003	Orange
0x04560006	SPM Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560003	Red
0x04560007	SPM Threshold Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x04560003	N/A
0x04560008	SPM Test Creation Event	RTM_Test	None	N/A
0x0456000a	SPM Test Modification Event	RTM_Test	None	N/A
0x0456000b	SPM Packet Loss Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x0456000c	SPM Packet Loss Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456000b	Yellow
0x0456000d	SPM Packet Loss Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456000b	Orange
0x0456000e	SPM Packet Loss Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456000b	Red
0x0456000f	SPM Packet Loss Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x0456000b	N/A
0x04560010	SPM Result Event (Jitter)	RTM_Test	None	N/A

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x04560011	SPM Jitter Packet Loss Source to Destination Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x04560012	SPM Jitter Packet Loss Source to Destination Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560011	Yellow
0x04560013	SPM Jitter Packet Loss Source to Destination Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560011	Orange
0x04560014	SPM Jitter Packet Loss Source to Destination Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560011	Red
0x04560015	SPM Jitter Packet Loss Source to Destination Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x04560011	N/A
0x04560016	SPM Jitter Packet Loss Destination to Source Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x04560017	SPM Jitter Packet Loss Destination to Source Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560016	Yellow
0x04560018	SPM Jitter Packet Loss Destination to Source Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560016	Orange
0x04560019	SPM Jitter Packet Loss Destination to Source Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560016	Red
0x0456001a	SPM Jitter Packet Loss Destination to Source Threshold Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x04560016	N/A

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x0456001b	SPM Jitter Packet MIA Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x0456001c	SPM Jitter Packet MIA Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456001b	Yellow
0x0456001d	SPM Jitter Packet MIA Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456001b	Orange
0x0456001e	SPM Jitter Packet MIA Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456001b	Red
0x0456001f	SPM Jitter Packet MIA Threshold Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x0456001b	N/A
0x04560020	SPM Jitter Packet Late Arrival Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x04560021	SPM Jitter Packet Late Arrival Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560020	Yellow
0x04560022	SPM Jitter Packet Late Arrival Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560020	Orange
0x04560023	SPM Jitter Packet Late Arrival Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560020	Red
0x04560024	SPM Jitter Packet Late Arrival Threshold Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x04560020	N/A
0x04560025	SPM Jitter Busies Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x04560026	SPM Jitter Busies Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560025	Yellow
0x04560027	SPM Jitter Busies Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560025	Orange
0x04560028	SPM Jitter Busies Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560025	Red
0x04560029	SPM Jitter Busies Threshold Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x04560025	N/A
0x0456002a	SPM Test Pause (Test Host Down) Event	RTM_Test	None	N/A
0x0456002b	SPM Test Restart (Test Host Recontacted) Event	RTM_Test	None	N/A
0x0456002c	SPM Test Entering Management Mode Event	RTM_Test	None	N/A
0x0456002d	SPM Test Exiting Management Mode Event	RTM_Test	None	N/A
0x0456002e	SPM Result Event (HTTP)	RTM_Test	None	N/A
0x0456002f	SPM HTTP DNS Resolution Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x04560030	SPM HTTP DNS Resolution Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456002f	Yellow
0x04560031	SPM HTTP DNS Resolution Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456002f	Orange

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x04560032	SPM HTTP DNS Resolution Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456002f	Red
0x04560033	SPM HTTP DNS Resolution Threshold Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x0456002f	N/A
0x04560034	SPM HTTP TCP Connect Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x04560035	SPM HTTP TCP Connect Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560034	Yellow
0x04560036	SPM HTTP TCP Connect Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560034	Orange
0x04560037	SPM HTTP TCP Connect Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560034	Red
0x04560038	SPM HTTP TCP Connect Threshold Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x04560034	N/A
0x04560039	SPM HTTP Page Download Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x0456003a	SPM HTTP Page Download Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456003c	Yellow
0x0456003b	SPM HTTP Page Download Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456003c	Orange
0x0456003c	SPM HTTP Page Download Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456003c	Red

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x0456003d	SPM HTTP Page Download Threshold Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x0456003c	N/A
0x0456003e	SPM Result Event (Traceroute)	RTM_Test	None	N/A
0x0456003f	SPM Traceroute Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x04560040	SPM Traceroute Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456003f	Yellow
0x04560041	SPM Traceroute Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456003f	Orange
0x04560042	SPM Traceroute Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456003f	Red
0x04560043	SPM Traceroute Threshold Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x0456003f	N/A
0x04560044	SPM Test SNMP Set Failure Event	RTM_TestHost	0x04560044	Yellow
0x04560045	SPM Test SNMP Set Failure Cleared Event	RTM_TestHost	Clears 0x04560044	N/A
0x04560046	SPM Test Timeout Cleared Event	RTM_Test	Clears 0x04560001	N/A
0x04560047	SPM Test Host Configuration Failed Cleared Event	RTM_Test	Clears 0x04560002	N/A
0x04560048	SPM Too Many Probes On Test Host Event	RTM_TestHost	0x04560048	Yellow

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x04560049	SPM Too Many Probes on Test Host Cleared Event	RTM_TestHost	Clears 0x04560048	N/A
0x0456004a	SPM HTTP Result Event	RTM_Test	None	N/A
0x04560054	Bad Ping Result	RTM_Test	None	N/A
0x04560055	Bad Jitter Result	RTM_Test	None	N/A
0x04560056	Bad HTTP Result	RTM_Test	None	N/A
0x04560057	Bad Traceroute Result	RTM_Test	None	N/A
0x04560058	Bad HTTP Result	RTM_Test	None	N/A
0x04560059	SPM Test No Longer On Device Event	RTM_Test	0x04560059	Yellow
0x0456005a	SPM Test No Longer Running On Device Event	RTM_Test	None	N/A
0x0456005b	SPM Duplicate Result Event	RTM_Test	None	N/A
0x0456005c	SPM Test Discovery Completion Event	RTM_TestHost	None	N/A
0x0456005d	SPM Test Type Mismatch Event	RTM_Test	0x0456005d	Yellow
0x0456005e	SPM Stale Test Cleared Event	RTM_Test	Clears 0x04560059 0x0456005d	N/A
0x0456005f	SPM Positive Jitter Source to Destination Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x04560060	SPM Positive Jitter Source to Destination Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456005f	Yellow

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x04560061	SPM Positive Jitter Source to Destination Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456005f	Orange
0x04560062	SPM Positive Jitter Source to Destination Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456005f	Red
0x04560063	SPM Positive Jitter Source to Destination Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x0456005f	N/A
0x04560064	SPM Positive Jitter Destination to Source Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x04560065	SPM Positive Jitter Destination to Source Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560064	Yellow
0x04560066	SPM Positive Jitter Destination to Source Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560064	Orange
0x04560067	SPM Positive Jitter Destination to Source Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560064	Red
0x04560068	SPM Positive Jitter Destination to Source Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x04560064	N/A
0x04560069	SPM Negative Jitter Source to Destination Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x0456006a	SPM Negative Jitter Source to Destination Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560069	Yellow

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x0456006b	SPM Negative Jitter Source to Destination Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560069	Orange
0x0456006c	SPM Negative Jitter Source to Destination Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560069	Red
0x0456006d	SPM Negative Jitter Source to Destination Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x04560069	N/A
0x0456006e	SPM Negative Jitter Destination to Source Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x0456006f	SPM Negative Jitter Destination to Source Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456006e	Yellow
0x04560070	SPM Negative Jitter Destination to Source Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456006e	Orange
0x04560071	SPM Negative Jitter Destination to Source Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456006e	Red
0x04560072	SPM Negative Jitter Destination to Source Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x0456006e	N/A
0x04560073	SPM Too Many Probes Event	RTM_Test	None	N/A
0x04560074	SPM Bad Community String Event	RTM_Test	None	N/A

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x04560075	SPM Invalid Destination Address Event	RTM_Test	0x04560075	Yellow
0x04560076	SPM Invalid Destination Address Cleared Event	RTM_Test	Clears 0x04560075	N/A
0x04560077	SPM Invalid Test Host Event	RTM_Test	0x04560077	Yellow
0x04560078	SPM Invalid Test Type Event	RTM_Test	0x04560078	Yellow
0x04560079	SPM RTM_TestHost No Device Model Event	RTM_TestHost	0x04560079	Yellow
0x0456007a	SPM RTM_TestHost No Device Model Cleared Event	RTM_TestHost	Clears 0x04560079	N/A
0x0456007b	SPM Result Failure Event	RTM_Test	None	N/A
0x0456007c	SPM Mean Opinion Score (MOS) event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x0456007d	SPM Mean Opinion Score (MOS) event	RTM_Test, RTM_TestHost, Source, or Destination	0x456007c	Yellow
0x0456007e	SPM Mean Opinion Score (MOS) event	RTM_Test, RTM_TestHost, Source, or Destination	0x456007c	Orange
0x0456007f	SPM Mean Opinion Score (MOS) event	RTM_Test, RTM_TestHost, Source, or Destination	0x456007c	Red
0x04560080	SPM Mean Opinion Score (MOS) event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x456007c	N/A
0x04560081	Juniper Jitter Result Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x04560082	Bad Juniper Jitter Result	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x04560083	Juniper RTT Jitter Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x04560084	Juniper RTT Jitter Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560083	Yellow
0x04560085	Juniper RTT Jitter Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560083	Orange
0x04560086	Juniper RTT Jitter Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560083	Red
0x04560087	Juniper RTT Jitter Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560083	N/A
0x04560088	Juniper Egress Jitter Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x04560089	Juniper Egress Jitter Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560088	Yellow
0x0456008a	Juniper Egress Jitter Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560088	Orange
0x0456008b	Juniper Egress Jitter Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560088	Red
0x0456008c	Juniper Egress Jitter Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x04560088	N/A

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x0456008d	Juniper Egress Jitter Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x0456008e	Juniper Egress Jitter Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456008d	Yellow
0x0456008f	Juniper Egress Jitter Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456008d	Orange
0x04560090	Juniper Egress Jitter Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456008d	Red
0x04560091	Juniper Egress Jitter Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x0456008d	N/A
0x04560092	ICMP_Jitter Result Event	RTM_Test	None	N/A
0x04560093	SPM ICMP_Jitter Bad Result Event	RTM_Test	None	N/A
0x04560094	SPM ICMP_Jitter Packet out of sequence source to destination Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x04560095	SPM ICMP_Jitter Packet out of sequence source to destination Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560094	Yellow
0x04560096	SPM ICMP_Jitter Packet out of sequence source to destination Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560094	Orange

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x04560097	SPM ICMP_Jitter Packet out of sequence source to destination Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560094	Red
0x04560098	SPM ICMP_Jitter Packet out of sequence source to destination Threshold Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x04560094	N/A
0x04560099	SPM ICMP_Jitter Packet out of sequence destination to source Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x0456009a	SPM ICMP_Jitter Packet out of sequence destination to source Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560099	Yellow
0x0456009b	SPM ICMP_Jitter Packet out of sequence destination to source Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560099	Orange
0x0456009c	SPM ICMP_Jitter Packet out of sequence destination to source Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560099	Red

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x0456009d	SPM ICMP_Jitter Packet out of sequence destination to source Threshold Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x04560099	N/A
0x0456009e	SPM Jitter Packet Out of Sequence BOTH Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x0456009f	SPM Jitter Packet Out of Sequence BOTH Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456009e	Yellow
0x04560100	SPM Jitter Packet Out of Sequence BOTH Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456009e	Orange
0x04560101	SPM Jitter Packet Out of Sequence BOTH Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x0456009e	Red
0x04560102	SPM Jitter Packet Out Of Sequence BOTH Threshold Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x0456009e	N/A
0x04560103	SPM Jitter Packet Skipped Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	None	N/A
0x04560104	SPM Jitter Packet Skipped Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560103	Yellow
0x04560105	SPM Jitter Packet Skipped Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560103	Orange
0x04560106	SPM Jitter Packet Skipped Threshold Exceeded Event	RTM_Test, RTM_TestHost, Source, or Destination	0x04560103	Red

Event Code	Event Name	Model Type Asserted On	Alarm Generated or Cleared	Alarm Severity
0x04560107	SPM Jitter Packet Skipped Threshold Cleared Event	RTM_Test, RTM_TestHost, Source, or Destination	Clears 0x04560103	N/A

Index