



Service Assurance Agent Enhancements



Note

The Service Assurance (SA) Agent is a new name for the Response Time Reporter (RTR) feature. The command line interface for the feature does not reflect the name change; commands retain the RTR name. Unless otherwise noted, RTR commands retain the functionality of earlier Cisco IOS releases.

This feature module describes the SA Agent Enhancements feature. It includes information on the benefits of the new feature, supported platforms and related documents.

This document contains the following sections:

- Feature Overview, page 1
- Supported Platforms, page 2
- Supported Standards, MIBs, and RFCs, page 3
- Configuration Tasks, page 3
- Monitoring and Maintaining the SA Agent, page 8
- Configuration Examples, page 9
- Command Reference, page 11
- Glossary, page 33

Feature Overview

The SA Agent is an both an enhancement to and a new name for the Response Time Reporter (RTR) feature that was introduced in Cisco IOS release 11.2. The feature allows you to monitor network performance between a Cisco router and a remote device (which can be another Cisco router, an IP host, or a mainframe host) by measuring key Service Level Agreement (SLA) metrics such as response time, network resources, availability, jitter, connect time, packet loss, and application performance. This feature enables you to perform troubleshooting, problem analysis, and notification based on the statistics collected by the SA Agent.

The SA Agent Enhancements feature introduces new performance measurement operations and enhancements to assist in the measurement of SLAs. With Cisco IOS release 12.1(1)T, the SA Agent provides new capabilities that enable you to:

- Measure FTP file download response time using the new file transfer protocol (FTP) operation
- Monitor one-way latency reporting through enhancements to the jitter operation

- Configure a new option for the Dynamic Host Configuration Protocol (DHCP) operation
- Manually enable a responder port
- Verify data for the udpEcho operation
- Configure new options for the **rtr schedule** command
- Restart an operation

Benefits

The SA Agent Enhancements feature enhances the management and measurement of enterprise and service provider networks. SLAs are useful for managed network services such as managed WAN access and managed virtual private network (VPN) services. The SA Agent Enhancement feature provides tools for measuring network performance using FTP, which is one of the most popular traffic types in Internet service provider (ISP) networks, and jitter (one-way delay), which is important for applications such as Voice over IP (VoIP).

Related Features and Technologies

The SA Agent feature module is related to the existing RTR feature, which is documented in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Related Documents

- *Cisco IOS Release 12.1 Configuration Fundamentals Configuration Guide*
- *Cisco IOS Release 12.1 Configuration Fundamentals Command Reference*

Supported Platforms

- Cisco 1000 series routers
- Cisco 1400 series routers
- Cisco 1600 series routers
- Cisco 1700 series routers
- Cisco 2500 series routers
- Cisco 2600 series routers
- Cisco 3600 series access servers and routers
- Cisco 3800 series routers
- Cisco 4000/m series routers
- Cisco 4500 series routers
- Cisco 4700 series routers
- Cisco 6400 series routers
- Cisco 7200 series routers

- Cisco 7500 series routers
- Cisco uBR7200 series cable routers
- Cisco AS5200, AS5300, and AS5800 access servers
- Cisco 12000 series gigabit switch router

Supported Standards, MIBs, and RFCs

Standards

No standards are supported by this feature.

MIBs

The SA Agent supports the Cisco Round Trip Time Monitor (RTTMON) MIB and the following MIB enhancements:

- Addition of rttMonAuthTable which allows the user to configure authentication strings
- Extensions of the rttMonJitterStatsTable and rttMonLatestJitterOperTable
- Addition of rttMonEchoAdminMode for FTP operation
- Extension of rttMonAppl table which allows the user to enable the SA Agent responder using the MIB

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

No RFCs are supported by this feature.

Configuration Tasks

See the following sections for configuration tasks for the SA Agent Enhancements feature. Refer to the Command Reference section for detailed syntax descriptions of the commands used in these tasks. Each task in the list indicates if the task is optional or required.

- Configuring the Operation, page 3 (Required)
- Configuring Optional Operation Characteristics, page 5 (Optional)
- Scheduling the Operation, page 6 (Required)
- Verifying SA Agent, page 6 (Optional)

Configuring the Operation

Response time and availability information is collected by *operations* (formerly known as probes) that you configure on a Cisco device such as a router or access server. Operations use synthetic packets specifically placed in a network to collect data about the network. These packets simulate other forms of network traffic, as determined by the type of operation you configure. SA Agent operations are given

specific identification numbers so you can track the various operations you configure and execute. SA Agent operations are configured in RTR configuration mode. You must configure the operation type before you can configure any of the other characteristics.

See the following sections for tasks for configuring the operation for the SA Agent Enhancements feature:

- Configuring an FTP Operation, page 4
- Configuring a DHCP Operation, page 4
- Configuring a One-way Delay Report Using a Jitter Operation, page 4
- Configuring the SA Agent Responder, page 5

Configuring an FTP Operation

To define an FTP operation, use the following commands starting in global configuration mode:

	Command	Purpose
Step 1	Router(config)# rtr <i>operation_id</i>	Specifies an operation and enters SA Agent configuration mode.
Step 2	Router(config-rtr)# type ftp operation <i>operation-type</i> url <i>url</i> [source-addr <i>source-addr</i>] [mode { <i>passive</i> <i>active</i> }]	Uses an FTP get request to download a file from a remote server.

Configuring a DHCP Operation

To define a DHCP operation, use the following commands starting in global configuration mode:

	Command	Purpose
Step 1	Router(config)# rtr <i>operation_id</i>	Specifies an operation and enters SA Agent configuration mode.
Step 2	Router(config-rtr)# type dhcp [source-ipaddr <i>source-ipaddr</i>] [dest-ipaddr <i>dest-ipaddr</i>] [option <i>decimal-option</i>] [circuit-id] [remote-id] [subnet-mask]	Defines a DHCP operation.

Configuring a One-way Delay Report Using a Jitter Operation



Note

To accurately measure one-way delay between two devices, you must synchronize the clocks on each device. To synchronize the clocks on each device, you must configure the Cisco IOS Network Time Protocol feature on both the source and destination devices.



Note

If the sum of the source to destination (SD) and the destination to source (DS) values is not within 10 percent of the round-trip time, the one-way measurement value is discarded.

To define a jitter operation with one-way delay reporting, use the following commands starting in global configuration mode:

	Command	Purpose
Step 1	Router(config)# rtr <i>operation_id</i>	Specifies an operation and enters SA Agent configuration mode.
Step 2	Router(config-rtr)# type jitter dest-ipaddr {name ipaddr} dest-port port-number [source-ipaddr {name ipaddr}] [source-port port-number] [control {enable disable}] [num-packets number-packets] [interval inter-packet-interval]	Defines a jitter operation.

Configuring the SA Agent Responder

To enable SA Agent Responder functionality, use the following command starting in global configuration mode:

Command	Purpose
Router(config-rtr)# rtr responder [type protocol [ipaddr ipaddr] { port port}]	Enables SA Agent Responder functionality on a device.

Configuring Optional Operation Characteristics

See the following sections for tasks for configuring the optional operation characteristics for the SA Agent Enhancements feature:

- Verifying Data for the udpEcho Operation, page 5
- Specifying the data pattern in udpEcho packets, page 5

Verifying Data for the udpEcho Operation

To verify data for a udpEcho operation, use the following command in global configuration mode:

Command	Purpose
Router(config)# rtr <i>operation_id</i>	Specifies an operation and enters SA Agent configuration mode.
Router(config-rtr)# verify-data	Enables data verification for udpEcho.

Specifying the data pattern in udpEcho packets

To specify the data pattern for a udpEcho operation, use the following command in global configuration mode:

Command	Purpose
Router(config)# rtr <i>operation_id</i>	Specifies an operation and enters SA Agent configuration mode.
Router(config-rtr)# data-pattern <i>hex-pattern</i>	Specifies the data pattern for a udpEcho operation.

Scheduling the Operation

Operations can be configured and not executed. In order to execute an operation, you must schedule it.

To schedule and restart an operation, use the following commands starting in global configuration mode:

	Command	Purpose
Step 1	Router(config)# rtr <i>operation_id</i>	Specifies an operation and enters SA Agent configuration mode.
Step 2	Router(config-rtr)# rtr schedule <i>operation-id</i> [life { forever <i>seconds</i> }] [start-time { pending now after <i>hh:mm:ss</i> <i>hh:mm</i> [month day day month] <i>hh:mm:ss</i> [month day day month]}] [ageout <i>seconds</i>]	Specifies the operation by configuring the time parameters.
Step 3	Router(config-rtr)# rtr restart <i>operation-id5</i>	Restarts an operation.

Verifying SA Agent

To verify that the SA Agent feature is configured properly, use the following commands:

- **show rtr application**
- **show rtr collection-statistics**
- **show rtr operational-state**
- **show rtr configuration**

The following example verifies how many operations are running.

```

router# show rtr application
    Response Time Reporter
Version:2.1.0 Round Trip Time MIB
Max Packet Data Size (ARR and Data):16384
Time of Last Change in Whole RTR:*22:37:12.000 UTC Sat Mar 6 1993
System Max Number of Entries:500

Number of Entries configured:5
    Number of active Entries:5
    Number of pending Entries:0
    Number of inactive Entries:0

Supported Operation Types
Type of Operation to Perform: echo
Type of Operation to Perform: pathEcho
Type of Operation to Perform: udpEcho
Type of Operation to Perform: tcpConnect
Type of Operation to Perform: http
Type of Operation to Perform: dns

```

```
Type of Operation to Perform: jitter
Type of Operation to Perform: dlsw
Type of Operation to Perform: dhcp
```

```
Supported Protocols
Protocol Type:ipIcmpEcho
Protocol Type:ipUdpEchoAppl
Protocol Type:ipTcpConn
Protocol Type:httpAppl
Protocol Type:dnsAppl
Protocol Type:jitterAppl
Protocol Type:dhcp
```

Number of configurable probe is 490

The following example verifies that the statistics are being collected for an HTTP operation:

```
router# show rtr collection-statistics
Collected Statistics

Entry Number:1
HTTP URL:http://172.20.150.200
Start Time:*00:01:16.000 UTC Mon Mar 1 1993

Comps:1           RTTMin:343
OvrTh:0           RTTMax:343
DNSTimeOut:0      RTTSum:343
TCPTimeOut:0      RTTSum2:117649
TraTimeOut:0      DNSRTT:0
DNSError:0        TCPConRTT:13
HTTPError:0       TransRTT:330
IntError:0        MesgSize:1771
Busies:0
```

The following example verifies that the operations are running:

```
router# show rtr operational-state
Current Operational State
Entry Number:3
Modification Time:*22:15:43.000 UTC Sat Mar 6 1993
Diagnostics Text:
Last Time this Entry was Reset:Never
Number of Octets in use by this Entry:1332
Number of Operations Attempted:2
Current Seconds Left in Life:3511
Operational State of Entry:active
Latest Completion Time (milliseconds):544
Latest Operation Start Time:*22:16:43.000 UTC Sat Mar 6 1993
Latest Oper Sense:ok
Latest Sense Description:200 OK
Total RTT:544
DNS RTT:12
TCP Connection RTT:28
HTTP Transaction RTT:504
HTTP Message Size:9707
```

The following example verifies that the SA Agent is configured:

```
router# show rtr configuration
Complete Configuration Table (includes defaults)
Entry Number:3
Owner:Joe
Tag:AppleTree
Type of Operation to Perform:http
```

```

Reaction and History Threshold (milliseconds):5000
Operation Frequency (seconds):60
Operation Timeout (milliseconds):5000
Verify Data:FALSE
Status of Entry (SNMP RowStatus):active
Protocol Type:httpAppl
Target Address:
Source Address:0.0.0.0
Target Port:0
Source Port:0
Request Size (ARR data portion):1
Response Size (ARR data portion):1
Control Packets:enabled
Loose Source Routing:disabled
LSR Path:
Type of Service Parameters:0x0
HTTP Operation:get
HTTP Server Version:1.0
URL:http://www.cisco.com
Cache Control:enabled
Life (seconds):3600
Next Scheduled Start Time:Start Time already passed
Entry Ageout:never
Connection Loss Reaction Enabled:FALSE
Timeout Reaction Enabled:FALSE
Threshold Reaction Type:never
Threshold Falling (milliseconds):3000
Threshold Count:5
Threshold Count2:5
Reaction Type:none
Number of Statistic Hours kept:2
Number of Statistic Paths kept:1
Number of Statistic Hops kept:1
Number of Statistic Distribution Buckets kept:1
Statistic Distribution Interval (milliseconds):20
Number of History Lives kept:0
Number of History Buckets kept:15
Number of History Samples kept:1
History Filter Type:none

```

Monitoring and Maintaining the SA Agent

To monitor the jitter one-way delay measurements, use the following commands:

- **show rtr operational-state**
- **show rtr collection-statistics**

The following example verifies that a one-way delay report jitter operation is running:

```

rtr7# show rtr operational-state
Current Operational State
Entry Number: 1
Modification Time: 11:12:02.000 UTC Thu Jul 1 1999
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1370
Number of Operations Attempted: 52
Current Seconds Left in Life: 9996936
Operational State of Entry: active
Latest Operation Start Time: 12:03:03.000 UTC Thu Jul 1 1999
RTT Values:

```

```

NumOfRTT: 10  RTTSum: 75  RTTSum2: 571
Packet Loss Values:
PacketLossSD: 0  PacketLossDS: 0
PacketOutOfSequence: 0  PacketMIA: 0  PacketLateArrival: 0
InternalError: 0  Busies:0
Jitter Values:
MinOfPositivesSD: 2  MaxOfPositivesSD: 2
NumOfPositivesSD: 1  SumOfPositivesSD: 2  Sum2PositivesSD: 4
MinOfNegativesSD: 0  MaxOfNegativesSD: 0
NumOfNegativesSD: 0  SumOfNegativesSD: 0  Sum2NegativesSD: 0
MinOfPositivesDS: 1  MaxOfPositivesDS: 1
NumOfPositivesDS: 2  SumOfPositivesDS: 2  Sum2PositivesDS: 2
MinOfNegativesDS: 1  MaxOfNegativesDS: 1
NumOfNegativesDS: 1  SumOfNegativesDS: 1  Sum2NegativesDS: 1
One Way Values:
NumOfOW: 10
OWMinSD: 3  OWMaxSD: 5  OWSumSD: 48  OWSum2SD: 234
OWMinDS: 2  OWMaxDS: 3  OWSumDS: 27  OWSum2DS: 75

```

The following example verifies that the statistics are being collected for a one-way delay report using a jitter operation:

```

rtr7# show rtr collection-statistics
Collected Statistics

Entry Number: 1
Target Address: 5.0.0.1, Port Number:99
Start Time: 11:12:03.000 UTC Thu Jul 1 1999
RTT Values:
NumOfRTT: 600  RTTSum: 3789  RTTSum2: 138665
Packet Loss Values:
PacketLossSD: 0  PacketLossDS: 0
PacketOutOfSequence: 0  PacketMIA: 0  PacketLateArrival: 0
InternalError: 0  Busies: 0
Jitter Values:
MinOfPositivesSD: 1  MaxOfPositivesSD: 2
NumOfPositivesSD: 26  SumOfPositivesSD: 31  Sum2PositivesSD: 41
MinOfNegativesSD: 1  MaxOfNegativesSD: 4
NumOfNegativesSD: 56  SumOfNegativesSD: 73  Sum2NegativesSD: 133
MinOfPositivesDS: 1  MaxOfPositivesDS: 338
NumOfPositivesDS: 58  SumOfPositivesDS: 409  Sum2PositivesDS: 114347
MinOfNegativesDS: 1  MaxOfNegativesDS: 338
NumOfNegativesDS: 48  SumOfNegativesDS: 396  Sum2NegativesDS: 114332
One Way Values:
NumOfOW: 440
OWMinSD: 2  OWMaxSD: 6  OWSumSD: 1273  OWSum2SD: 4021
OWMinDS: 2  OWMaxDS: 341  OWSumDS: 1643  OWSum2DS: 120295

```

Configuration Examples

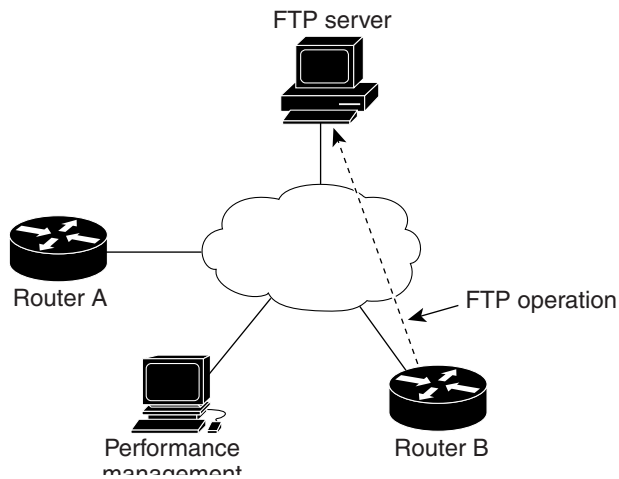
This section provides the following configuration examples:

- Configuring an FTP Operation, page 10
- Configuring a DHCP Operation Specifying Option 82, page 10
- Configuring the SA Agent Responder, page 10

Configuring an FTP Operation

An FTP operation is configured as shown in Figure 1.

Figure 1 FTP Operation



In the following example, SA Agent operation 20 is configured as an FTP operation. ira is the user, smith is the password, zxq is the host name or address, and test is the file name.

```
(config)# rtr 20
(config-rtr)# ftp://ira:smith@zxq/test
```

Configuring a DHCP Operation Specifying Option 82

In the following example, SA Agent operation number 4 is configured as a DHCP operation enabled for DHCP server 172.16.20.3:

```
(config)# rtr 4
(config-rtr)# type dhcp option 82 circuit-id 10005A6F1234
(config)# ip dhcp-server 172.16.20.3
```

Configuring the SA Agent Responder

The following example enables the SA Responder:

```
rtr responder
```

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the *Cisco IOS Release 12.1 Configuration Fundamentals Command Reference*.

- **data-pattern**
- **rtr reaction-configuration**
- **rtr responder**
- **rtr restart**
- **rtr schedule**
- **show rtr collection-statistics**
- **show rtr operational-state**
- **type dhcp**
- **type ftp operation**

data-pattern

To specify the data pattern in a udpEcho packet, use the **data pattern** RTR configuration mode command. To remove the data pattern specification, use the **no** form of this command.

data-pattern *hex-pattern*

no data-pattern *hex-pattern*

Syntax Description	<i>hex-pattern</i>	udpEcho packet pattern display, in hexadecimal. The hexadecimal range is 0 to F.
Defaults	The default is ABCD.	
Command Modes	RTR configuration	
Command History	Release	Modification
	12.1(1)T	This command was introduced.
Usage Guidelines	The data-pattern command is applicable to the udpEcho operation, only.	
Examples	The following example specifies 1234ABCD5678 as the data pattern:	
	<pre>rtr 1 type udpEcho dest-ipaddr 10.0.54.205 dest-port 101 data-pattern 1234ABCD5678</pre>	
Related Commands	Command	Description
	show rtr configuration	Displays configuration values including all defaults for all SA Agent operations or the specified operation.
	show rtr collection-statistics	Displays statistical errors for all SA Agent operations or the specified operation.

rtr reaction-configuration

To configure certain actions to occur based on events under the control of the SA Agent, use the **rtr reaction-configuration** global configuration command. Use the **no** form of this command to return to the default values of the operation.

```
rtr reaction-configuration operation [verify-error-enable] [connection-loss-enable]
[timeout-enable] [threshold-falling milliseconds] [threshold-type option] [action-type
option]
```

```
no rtr reaction-configuration operation
```

Syntax	Description
<i>operation</i>	Number of the SA Agent operation to configure.
verify-error-enable	(Optional) Enables error verification. The default is disabled.
connection-loss-enable	(Optional) Enables checking for connection loss in connection-oriented protocols. The default is disabled.
timeout-enable	(Optional) Enables checking for response time reporting operation timeouts based on the timeout value configured for the operation with the timeout RTR configuration command. The default is disabled.
threshold-falling <i>milliseconds</i>	(Optional) Sets the falling threshold (standard RMON-type hysteresis mechanism) in milliseconds. When the falling threshold is met, generates a resolution reaction event. The rising of the operation over threshold is set with the threshold RTR configuration command. The default value is 3000 ms.

-
- threshold-type** *option* (Optional) Specifies the algorithm used by the SA Agent to calculate over and falling threshold violations. Option can be one of the following keywords:
- **never**—Do not calculate threshold violations. This is the default.
 - **immediate**—When the response time exceeds the rising over threshold or drops below the falling threshold, immediately perform the action defined by **action-type**.
 - **consecutive** [*occurrences*]—When the response time exceeds the rising threshold consecutively five times or drops below the falling threshold consecutively five times, perform the action defined by **action-type**. Optionally specify the number of consecutive occurrences. The default is 5.
 - **xofy** [*x-value y-value*]—When the response time exceeds the rising threshold five out of the last five times or drops below the falling threshold five out of the last five times, perform the action defined by **action-type**. Optionally specify the number of violations that must occur and the number that must occur within a specified number. The default is 5 for both x-value and y-value.
 - **average** [*attempts*]—When the average of the last five response times exceeds the rising threshold or when the average of the last five response times drops below the falling threshold, perform the action defined by **action-type**. Optionally specify the number of operations to average. The default is the average of the last five response time operations. For example: if the threshold of the operation is 5000 ms and the last three attempts results of the operation are 6000, 6000, and 5000 ms, the average would be $6000 + 6000 + 5000 = 17000/3 > 5000$, thus violating the 5000-ms threshold.
-

action-type <i>option</i>	<p>(Optional) Specify what action or combination of actions the operation performs when you configure connection-loss-enable or timeout-enable, or threshold events occur. For the action-type to occur for threshold events, the threshold-type must be defined to anything other than never. Option can be one of the following keywords:</p> <ul style="list-style-type: none"> • none—No action is taken. • trapOnly—Send an SNMP trap on both over and falling threshold violations. • nmvtOnly—Send an SNA NMVT Alert on over threshold violation and an SNA NMVT Resolution on falling threshold violations. • triggerOnly—Have one or more target operation’s operational state make the transition from “pending” to “active” on over (and falling) threshold violations. The target operations are defined with the rtr reaction-trigger command. A target operation will continue until its life expires as specified by the target operation’s life value configured with the rtr schedule global configuration command. A triggered target operation must finish its life before it can be triggered again. • trapAndNmvt—Send a combination of trapOnly and nmvtOnly. • trapAndTrigger—Send a combination of trapOnly and triggerOnly. • nmvtAndTrigger—Send a combination of nmvtOnly and triggerOnly. • trapNmvtAndTrigger—Send a combination of trapOnly, nmvtOnly, and triggerOnly.
----------------------------------	---

Defaults

No reactions are generated.
 Error verification is disabled.
 Connection loss is disabled.
 Checking the timeout is disabled.
 The falling threshold value is 3000 ms.
 The algorithm threshold is **never**.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	The verify-error-enable optional keyword was added.

Usage Guidelines

Triggers are used for diagnostics purposes and are not used in normal operation.
 You can use triggers to assist you in determining where delays are happening in the network when excessive delays are being seen on an end-to-end basis.

The reaction applies only to attempts to the target (that is, attempts to any hops along the path in **pathEcho** do not generate reactions).

**Note**

Keywords are not case sensitive and are shown in mixed case for readability only.

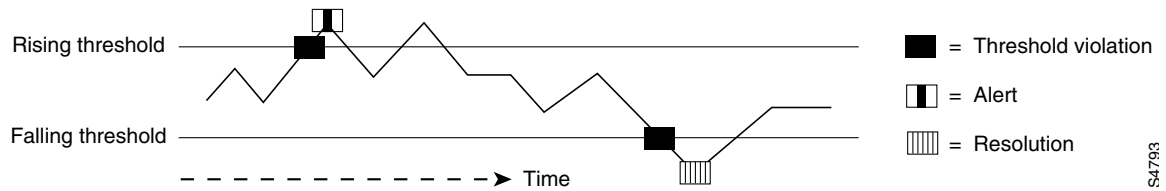
Examples

In the following example, operation 19 sends an SNMP trap when there is an over or falling threshold violation:

```
rtr reaction-configuration 19 threshold-type immediate action-type trapOnly
```

Figure 2 shows that an alert (rising trap) would be issued immediately when the response time exceeds the rising threshold and a resolution (falling trap) would be issued immediately when the response time drops below the falling threshold.

Figure 2 Example of Rising and Falling Thresholds



S4793

Related Commands

Command	Description
rtr	Specifies an SA Agent operation and enters RTR configuration mode.
rtr reaction-configuration	Defines a second SA Agent operation to make the transition from a pending state to an active state when one of the trigger action-type options are defined with the rtr reaction-configuration command.
threshold	Sets the rising threshold (hysteresis) that generates a reaction event and stores history information for the SA Agent operation.
timeout	Sets the amount of time the SA Agent operation waits for a response from its request packet.

rtr responder

To enable the SA Agent Responder feature on a target router, use the **rtr responder** global configuration command. Use the **no** form of this command to disable the SA Responder.

```
rtr responder [type protocol [ipaddr ipaddr] {port port}]
```

```
no rtr responder [type protocol [ipaddr ipaddr] {port port}]
```

Syntax Description

type	(Optional) Type of operation.
<i>protocol</i>	Protocol used by the operation. The applicable protocols are jitter, udpEcho, and tcpConnect.
ipaddr <i>ipaddr</i>	(Optional) IP address for the operation.
port <i>port</i>	Port number.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1(1)T	The type , ipaddr , and port keywords were added.

Usage Guidelines

This command is used on the intended target router of SA Agent operations to enable certain types of operations on non-native interfaces.

The **type**, **ipaddr**, and **port** keywords enable the SA Agent Responder to respond to probe packets without receiving control packets. The applicable protocols are jitter, udpEcho, and tcpConnect. The jitter operation will not compute packet loss because the SA Agent Responder does not know which probe packet has been received first.

Examples

The following example enables the SA Responder:

```
rtr responder
```

Related Commands

Command	Description
rtr	Specifies an SA Agent operation and enters RTR configuration mode.

rtr restart

To restart a SA Agent operation, use the **rtr restart** global configuration command.

rtr restart *operation-id*

Syntax Description

<i>operation-id</i>	Number (id) of the SA Agent operation to restart. SA Agent allows a maximum of 500 operations.
---------------------	--

Defaults

No default behavior or values.

Command Modes

Global configuration.

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

To restart an operation, the operation should be in active status.
 SA Agent allows a maximum of 500 operations.
 This command does not have a no form.

Examples

The following example restarts operation 12:

```
router(config)#rtr restart 12
```

rtr schedule

To configure the time parameters for an SA Agent operation, use the **rtr schedule** global configuration command. Use the **no** form of this command to stop the operation and restart it with the default parameters (that is, pending).

```
rtr schedule operation-id [life {forever | seconds}] [start-time {pending | now | after hh:mm:ss
| hh:mm [month day | day month] | hh:mm:ss [month day | day month]}] [ageout seconds]
```

```
no rtr schedule operation-id
```

Syntax Description	
<i>operation-id</i>	Number of the SA Agent operation to schedule.
life <i>seconds</i>	(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour).
forever	Schedule an operation to run indefinitely.
start-time	(Optional) Time when the operation starts collecting information. If the start-time is not specified, no information is collected until the start-time is configured or a trigger occurs that performs a start-time now .
pending	No information is collected. This is the default value.
now	Information is immediately collected.
after <i>hh:mm:ss</i>	(Optional) Schedule an operation to begin after a specified amount of time. Information is collected at the specified time (use a 24-hour clock).
<i>hh:mm</i>	Information is collected at the specified time (use a 24-hour clock). The time is the current day if you do not specify the month and day.
<i>month</i>	(Optional) Name of the month. If month is not specified, the current month is used. A day value is required.
<i>day</i>	(Optional) Number of the day in the range 1 to 31. If day is not specified, the current day is used. A month value is required.
<i>hh:mm:ss</i>	Information is collected at the specified time (use a 24-hour clock). The time is the current day if you do not specify the month and day.
<i>month</i>	(Optional) Name of the month. If month is not specified, the current month is used. A day value is required.
<i>day</i>	(Optional) Number of the day in the range 1 to 31. If day is not specified, the current day is used. A month value is required.
ageout <i>seconds</i>	(Optional) Number of seconds to keep the operation when it is not actively collecting information. The default is 0 seconds (never ages out).

Defaults

Place the operation in a pending state (that is, the operation is started but not actively collecting information).

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	The after and forever keywords were added.

Usage Guidelines

After you schedule the operation with the **rtr schedule** command, you cannot change the configuration of the operation (with the **rtr** global configuration command). To change the configuration of the operation, use the **no** form of the **rtr** global command and reenter the configuration information.

If the operation is in a pending state, you can define the conditions under which the operation makes the transition from pending to active with the **rtr reaction-trigger** and **rtr reaction-configuration** global configuration commands. When the operation is in an active state, it immediately begins collecting information.

The following time line shows the age-out process of the operation:

W-----X-----Y-----Z

Where:

- W is the time the operation was configured with the **rtr** global configuration command.
- X is the start time or start of life of the operation (that is, when the operation became “active”).
- Y is the end of life as configured with the **rtr schedule** global configuration command (life seconds have counted down to zero).
- Z is the age out of the operation.

Age out starts counting down at W and Y, is suspended between X and Y, and is reset to its configured size at Y.

It is possible for the operation to age out before it executes (that is, Z can occur before X). To ensure that this does not happen, the difference between the operation’s configuration time and start time (X and W) must be less than the age-out seconds.

**Note**

The total RAM required to hold the history and statistics tables is allocated at this time. This is to prevent router memory problems when the router gets heavily loaded and to lower the amount of overhead the feature causes on a router when it is active.

Examples

In the following example, operation 25 begins actively collecting data at 3:00 p.m. on April 5. This operation will age out after 12 hours of inactivity, which can be before it starts or after it has finished with its life. When this operation ages out, all configuration information for the operation is removed (that is, the configuration information is no longer in the running-config in RAM).

```
rtr schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

In the following example, operation 1 begins collecting data after a 5 minute delay:

```
rtr schedule 1 start after 00:05:00
```

In the following example, operation 3 begins collecting data immediately and is scheduled to run indefinitely:

```
rtr schedule 3 start-time now life forever
```

Related Commands	Command	Description
	rtr	Specifies an SA Agent operation and enters RTR configuration mode.
	rtr reaction-configuration	Configures certain actions to occur based on events under the control of the SA Agent.
	rtr reaction-trigger	Defines a second SA Agent operation to make the transition from a pending state to an active state when one of the trigger action-type options are defined with the rtr reaction-configuration command.

show rtr collection-statistics

To display statistical errors for all SA Agent operations or the specified operation, use the **show rtr collection-statistics EXEC** command.

show rtr collection-statistics [*operation*] [**tabular** | **full**]

Syntax Description		
	<i>operation</i>	(Optional) Number of the SA Agent operation to display.
	tabular	(Optional) Displays information in a column format reducing the number of screens required to display the information.
	full	(Optional) Displays all information using identifiers next to each displayed value. This is the default.

Defaults Full format for all operations. Shows statistics for the past two hours.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.0(5)T	The output for this command was expanded to show information for Jitter operations.
	12.1(1)T	The output for this command was expanded to show information for the FTP operation.

Usage Guidelines Use the **show rtr collection-statistics** command to display information such as the number of failed operations and the failure reason. You can also use the **show rtr distribution-statistics** and **show rtr totals-statistics** commands to display additional statistical information.

This command shows information collected over the past two hours, unless you specify a different amount of time using the **hours-of-statistics-kept** command.

Examples The following is sample output from the **show rtr collection-statistics** command in full format.

```
Router# show rtr collection-statistics 1

      Collected Statistics
Entry Number: 1
Start Time Index: *17:15:41.000 UTC Thu May 16 1996
Path Index: 1
Hop in Path Index: 1
Number of Failed Operations due to a Disconnect: 0
Number of Failed Operations due to a Timeout: 0
Number of Failed Operations due to a Busy: 0
Number of Failed Operations due to a No Connection: 0
Number of Failed Operations due to an Internal Error: 0
```

```

Number of Failed Operations due to a Sequence Error: 0
Number of Failed Operations due to a Verify Error: 0
Target Address: 172.16.1.176

```

The following example verifies that the statistics are being collected for an HTTP operation:

```

router# show rtr collection-statistics 2
      Collected Statistics

Entry Number:2
HTTP URL:http://172.20.150.200
Start Time:*00:01:16.000 UTC Mon Mar 1 1993

      Comps:1           RTTMin:343
      OvrTh:0           RTTMax:343
      DNSTimeOut:0      RTTSum:343
      TCPTimeOut:0      RTTSum2:117649
      TraTimeOut:0      DNSRTT:0
      DNSError:0        TCPConRTT:13
      HTTPError:0       TransRTT:330
      IntError:0        MesgSize:1771
      Busies:0

```

The following shows sample output from the **show rtr collection-statistics** command, where operation 1 is a Jitter operation:

**Note**

This example shows the one-way latency support that has been added to the jitter operation. To accurately measure one-way delay between two devices, you must synchronize the clocks on each device. To synchronize the clocks on each device, you must configure the Cisco IOS Network Time Protocol feature on both the source and destination devices.

**Note**

If the sum of the source to destination (SD) and the destination to source (DS) values is not within 10 percent of the round trip time, the one-way measurement value is discarded.

```

router# show rtr collection-statistics 1
      Collected Statistics

Entry Number: 1
Target Address: 5.0.0.1, Port Number:99
Start Time: 11:12:03.000 UTC Thu Jul 1 1999
RTT Values:
NumOfRTT: 600 RTTSum: 3789 RTTSum2: 138665
Packet Loss Values:
PacketLossSD: 0 PacketLossDS: 0
PacketOutOfSequence: 0 PacketMIA: 0 PacketLateArrival: 0
InternalError: 0 Busies: 0
Jitter Values:
MinOfPositivesSD: 1 MaxOfPositivesSD: 2
NumOfPositivesSD: 26 SumOfPositivesSD: 31 Sum2PositivesSD: 41
MinOfNegativesSD: 1 MaxOfNegativesSD: 4
NumOfNegativesSD: 56 SumOfNegativesSD: 73 Sum2NegativesSD: 133
MinOfPositivesDS: 1 MaxOfPositivesDS: 338
NumOfPositivesDS: 58 SumOfPositivesDS: 409 Sum2PositivesDS: 114347
MinOfNegativesDS: 1 MaxOfNegativesDS: 338
NumOfNegativesDS: 48 SumOfNegativesDS: 396 Sum2NegativesDS: 114332

```

```

One Way Values:
NumOfOW: 440
OWMinSD: 2  OWMaxSD: 6    OWSumSD: 1273  OWSum2SD: 4021
OWMinDS: 2  OWMaxDS: 341  OWSumDS: 1643  OWSum2DS: 120295

```

The values shown indicate the aggregated values for the current hour. RTT stands for Round-Trip-Time. SD stands for source-to-destination and represents the time from the source to the destination. DS stands for destination-to-source and represents the time from the destination to the source. Table 1 describes the significant fields shown in this output.

Table 1 *show rtr collection-statistics Field Descriptions*

Field	Description
NumOfRTT	Number of successful round trips.
RTTSum	Sum of those round trip values (in milliseconds).
RTTSum2	Sum of squares of those round trip values (in milliseconds).
PacketLossSD	Number of packets lost from source to destination.
PacketLossDS	Number of packets lost from destination to source.
PacketOutOfSequence	Number of packets returned out of order.
PacketMIA	Number of packets lost where the direction (SD/DS) cannot be determined.
PacketLateArrival	Number of packets that arrived after the timeout.
InternalError	Number of times an operation could not be started due to other internal failures.
Busies	Number of times this operation could not be started because the previously scheduled run was not finished.
MinOfPositivesSD MaxOfPositivesSD	Minimum and maximum positive jitter values from source to destination, in milliseconds.
NumOfPositivesSD	Number of jitter values from source to destination that are positive (in other words, network latency increases for two consecutive test packets).
SumOfPositivesSD	Sum of those positive values (in milliseconds).
Sum2PositivesSD	Sum of squares of those positive values.
MinOfNegativesSD MaxOfNegativesSD	Minimum and maximum negative jitter values from source to destination. The absolute value is given.
NumOfNegativesSD	Number of jitter values from source to destination that are negative (in other words, network latency decreases for two consecutive test packets).
SumOfNegativesSD	Sum of those values.
Sum2NegativesSD	Sum of the squares of those values.
One Way Value	Amount of time it took the packet to travel from the source router to the target router or from the target router to the source router.

Table 1 *show rtr collection-statistics Field Descriptions (continued)*

Field	Description
NumOfOW	Number of successful one-way time measurements.
OWMinSD	Minimum time from the source to the destination.
OWMaxSD	Maximum time from the source to the destination.
OWSumSD	Sum of those values.
OWSum2SD	Sum of the squares of those values.

The DS values show the same information as above for Destination-to-Source Jitter values.

Related Commands

Command	Description
show rtr configuration	Displays configuration values including all defaults for all SA Agent operations or the specified operation.
show rtr distributions-statistics	Displays statistic distribution information (captured response times) for all SA Agent operations or the specified operation.
show rtr totals-statistics	Displays the total statistical values (accumulation of error counts and completions) for all SA Agent operations or the specified operation.
show ntp status	Displays the status of the Network Time Protocol (NTP).

show rtr operational-state

To display the operational state of all SA Agent operations or the specified operation, use the **show rtr operational-state EXEC** command.

show rtr operational-state [*operation*] [**tabular** | **full**]

Syntax Description		
	<i>operation</i>	(Optional) Number of the SA Agent operation to display.
	tabular	(Optional) Display information in a column format reducing the number of screens required to display the information.
	full	(Optional) Display all information using identifiers next to each displayed value. This is the default.

Defaults Full format for all operations

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.0(5)T	This command was expanded to show information about Jitter operations.
	12.1(1)T	The output for this command was expanded to show information for the FTP operation.

Usage Guidelines Use the **show rtr operational-state** command to determine whether a connection loss, timeout, and over threshold occurred; how much life the operation has left; whether the operation is active; and the completion time. It also displays the results of the latest operation attempt.

Examples The following example shows sample output from the **show rtr operational-state** command in full format:

```
router# show rtr operational-state full
      Current Operational State
Entry Number:3
Modification Time:*22:15:43.000 UTC Sat Mar 6 1993
Diagnostics Text:
Last Time this Entry was Reset:Never
Number of Octets in use by this Entry:1332
Number of Operations Attempted:2
Current Seconds Left in Life:3511
Operational State of Entry:active
Latest Completion Time (milliseconds):544
Latest Operation Start Time:*22:16:43.000 UTC Sat Mar 6 1993
Latest Oper Sense:ok
Latest Sense Description:200 OK
Total RTT:544
```

```
DNS RTT:12
TCP Connection RTT:28
HTTP Transaction RTT:504
HTTP Message Size:9707
```

The following example shows sample output when the specified operation is a Jitter operation.

**Note**

This example shows the one-way latency support that has been added to the jitter operation. To accurately measure one-way delay between two devices, you must synchronize the clocks on each device. To synchronize the clocks on each device, you must configure the Cisco IOS Network Time Protocol feature on both the source and destination devices.

**Note**

If the sum of the source-to-destination (SD) and the destination-to-source (DS) values is not within 10 percent of the round trip time, the one-way measurement value is discarded.

```
router# show rtr operational-state 1
      Current Operational State
Entry Number:1
Modification Time: 11:12:02.000 UTC Thu Jul 1 1999
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1370
Number of Operations Attempted: 52
Current Seconds Left in Life: 9996936
Operational State of Entry: active
Latest Operation Start Time: 12:03:03.000 UTC Thu Jul 1 1999
RTT Values:
NumOfRTT: 10  RTTSum: 75  RTTSum2: 571
Packet Loss Values:
PacketLossSD: 0  PacketLossDS: 0
PacketOutOfSequence: 0  PacketMIA: 0  PacketLateArrival: 0
InternalError: 0  Busies:0
Jitter Values:
MinOfPositivesSD: 2  MaxOfPositivesSD: 2
NumOfPositivesSD: 1  SumOfPositivesSD: 2  Sum2PositivesSD: 4
MinOfNegativesSD: 0  MaxOfNegativesSD: 0
NumOfNegativesSD: 0  SumOfNegativesSD: 0  Sum2NegativesSD: 0
MinOfPositivesDS: 1  MaxOfPositivesDS: 1
NumOfPositivesDS: 2  SumOfPositivesDS: 2  Sum2PositivesDS: 2
MinOfNegativesDS: 1  MaxOfNegativesDS: 1
NumOfNegativesDS: 1  SumOfNegativesDS: 1  Sum2NegativesDS: 1
One Way Values:
NumOfOW: 10
OWMinSD: 3  OWMaxSD: 5  OWSumSD: 48  OWSum2SD: 234
OWMinDS: 2  OWMaxDS: 3  OWSumDS: 27  OWSum2DS: 75
```

The values shown indicate the values for the last SA Agent operation. RTT stands for Round-Trip-Time. SD stands for Source-to-Destination. DS stands for Destination-to-Source. For a description of the output fields, see Table 1 in the **show rtr collection-statistics** command documentation.

■ show rtr operational-state

Related Commands	Command	Description
	show rtr configuration	Displays configuration values including all defaults for all SA Agent operations or the specified operation.
	show ntp status	Displays the status of the Network Time Protocol (NTP).

type dhcp

To configure a Dynamic Host Configuration Protocol SA Agent operation, use the **type dhcp** RTR configuration command. To disable a DHCP SA Agent operation, use the **no** form of this command.

```
type dhcp [source-ipaddr source-ipaddr] [dest-ipaddr dest-ipaddr] [option decimal-option
  [circuit-id] [remote-id] [subnet-mask]]
```

```
no type dhcp
```

Syntax Description

source-ipaddr <i>source-ipaddr</i>	(Optional) Source name or IP address.
dest-ipaddr <i>dest-ipaddr</i>	(Optional) Destination name or IP address.
option <i>decimal-option</i>	(Optional) Option number. The only valid value is 82.
<i>circuit-id</i>	(Optional) Circuit ID in hexadecimal.
<i>remote-id</i>	(Optional) Remote ID in hexadecimal.
<i>subnet-mask</i>	(Optional) Subnet mask IP address. The default value is 255.255.255.0.

Defaults

The subnet-mask value is 255.255.255.0.

Command Modes

RTR configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(1)T	The following keywords were added: <ul style="list-style-type: none"> • source-ipaddr • dest-ipaddr • option

Usage Guidelines

You must configure the type of operation before you can configure any of the other characteristics of the operation.

If the source IP address is configured, then packets will be sent with that source address.

You may configure the **ip dhcp-server** command to identify the DHCP server that the DHCP operation will measure.

If the target IP address is configured, then only that device will be measured.

If the **ip dhcp-server** command is not configured and the target IP address is not configured, then DHCP discover packets will be sent on every available IP interface.

If an odd number of characters are specified for the *circuit-id*, a zero will be added to the end of the string.

Examples

In the following example, SA Agent operation number 4 is configured as a DHCP operation enabled for DHCP server 172.16.20.3:

```
(config)# rtr 4
(config-rtr)# type dhcp option 82 circuit-id 10005A6F1234
(config)# ip dhcp-server 172.16.20.3
```

Related Commands

Command	Description
rtr	Specifies an SA Agent operation and enters RTR configuration mode.
ip dhcp-server	Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.

type ftp operation

To configure an FTP operation, use the **type ftp operation** RTR configuration command. To remove the type configuration for the operation, use the **no** form of this command.

```
type ftp operation operation-type url url [source-ipaddr source-ipaddr] [mode {passive | active}]
```

```
no command type ftp operation
```

Syntax Description

<i>operation-type</i>	FTP operation. get is the only valid operation value.
url <i>url</i>	Location information for the file to retrieve.
source-ipaddr <i>source-ipaddr</i>	(Optional) Source address of the operation.
mode	(Optional) Specifies mode, either active or passive.
<i>passive</i>	Passive mode. This mode is the default.
<i>active</i>	Active mode.

Defaults

The default is passive mode.

Command Modes

RTR configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

Get is the only valid operation value. The URL must be in one of the following formats:

- ftp://user:password@host/filename
- ftp://host/filename

If the user and password keywords are not specified, the defaults are anonymous and test, respectively.

Examples

In the following example, an FTP operation is configured. Joe is the user and Young is the password. zxq is the host and test is the file name.

```
type ftp operation get ftp://joe:young@zxq/test
```

Related Commands

Command	Description
show rtr collection-statistics	Displays statistical errors for all SA Agent operations or the specified operation.
show rtr operational-state	Displays the operational state of all SA Agent operations or the specified operation.

Glossary

DHCP—Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

DNS—domain name server. System used in the Internet for translating names of network nodes into addresses.

Discover—A broadcast frame looking for DHCP server.

domain name server—See DNS.

Dynamic Host Configuration Protocol—See DHCP.

FTP—file transfer protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.

File Transfer Protocol—See FTP

HTTP—Hypertext Transfer Protocol. The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.

Hypertext Transfer Protocol—See HTTP.

ISP—Internet service provider. Company that provides Internet access to other companies and individuals.

Internet service provider—See ISP.

jitter—Jitter is the inter-packet delay variance; that is the difference between inter-packet arrival and departure. Jitter is an important QoS metric for voice and video applications.

lease—IP address that lasts a fixed amount of time.

NTP—Network Time Protocol. Protocol built on top of TCP that assures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

Network Time Protocol—See NTP.

operation—Test that measures network performance. See synthetic operation.

offer—Frame from a DHCP server with a proposed IP address for the client.

QoS—Quality of Service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

Quality of Service—See QoS.

RTR—Response Time Reporter. Cisco IOS feature that monitors network performance, network resources, and applications by measuring response times and availability. Also known as Service Assurance (SA) Agent.

response time reporter—See RTR.

Service Level Agreement—See SLA.

SLA—Agreement that specifies and guarantees minimum acceptable levels of service.

synthetic operation—Packets sent into the network that appear to be user data traffic but actually measure network performance. Formerly known as a probe. Also referred to as “operation.”

VoIP—Voice over IP. Enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In Voice over IP, the DSP segments the voice signal into frames, which are then coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.

VPN—Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

Virtual Private Network—See VPN.

Voice over IP—See VoIP.