



Network Monitoring Using Cisco Service Assurance Agent

This chapter describes how the Cisco Service Assurance Agent (formerly known as the Response Time Reporter) provides a variety of service monitoring information, including time-delay reporting using the Response Time Monitor MIB. The tasks in this chapter apply to Cisco IOS Release 12.1 and derivative releases.

For a complete description of the router monitoring commands mentioned in this chapter, refer to the “Cisco Service Assurance Agent Commands” chapter of the Release 12.1 [Cisco IOS Configuration Fundamentals Command Reference](#). To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Configuring Cisco Service Assurance Agent

The Cisco Service Assurance Agent (SAA) is an application-aware synthetic operation agent that monitors network performance by measuring key metrics such as response time, availability, jitter (interpacket delay variance), connect time, throughput, and packet loss. These metrics can be used for troubleshooting, for analysis before problems occur, and for designing future network topologies.

The Service Assurance Agent feature is both a new name for and an enhancement to the Response Time Reporter (RTR) feature introduced in Cisco IOS Release 11.2. The response time and availability monitoring capabilities of RTR have been extended to include support for Voice over IP (VoIP), quality of service (QoS), and the World Wide Web, and thus RTR has evolved into the SA Agent.



Note

Cisco SAA retains the use of **rtr** in the syntax for all CLI commands. Unless otherwise noted, RTR commands retain the functionality of earlier Cisco IOS releases. RTR is also used throughout the CLI in the output of **help** and **show** commands.

SAA is integrated into most feature-sets (system images) of Cisco IOS, and is available for all Cisco platforms which run IOS Release 12.0(5)T or later. It can be used via the CLI when the Cisco Response Time Monitoring (RTTMON) MIB is available to the router.



Note

You will need version 2.1.0 or later of the RTTMON MIB to use the features described in this chapter. For a complete description of the object variables referenced by the SAA feature, see the text of the CISCO-RTTMON-MIB file.

Because SAA is also accessible using SNMP, it can also be used by performance monitoring applications and Network Management Systems such as CiscoWorks2000 (CiscoWorks Blue) and the Internetwork Performance Monitor (IPM). SAA notifications can also be enabled via SNA NMVT for applications such as NetView.

The expanded functionality of SAA extends IP support and enhances the management and measurement of enterprise and service provider networks. With the increasing importance of mission-critical applications and networks that link global enterprises, customers are demanding service-level agreements (SLAs) that guarantee minimum acceptable levels of service. The Service Assurance Agent provides a reliable mechanism to accurately monitor and measure the key metrics in SLAs.

**Note**

The RTR concept of a probe has been expanded to include a variety of measurement operations used by the SAA feature. The terms *probe* and *operation* are used interchangeably for SAA operations in the documentation of this feature.

SAA Configuration Task List

To configure Cisco Service Assurance Agent, complete the tasks found in the following sections:

- Setting the Memory Threshold for SAA (Optional)
- Configuring SAA Operations (Required)
- Configuring the Operation Type (Required)
- Configuring SAA Operation Characteristics (Optional)
- Scheduling the Operation (Required)
- Enabling the SAA Responder on Operational Targets (Required for certain operations)
- Configuring SAA Control Message Authentication (Optional)
- Resetting the SAA (Optional)
- Viewing SAA Operational Results and SAA Status (Required)
- SAA Configuration Examples

Setting the Memory Threshold for SAA

To specify how much memory must be available on the router to allow SAA configuration, use the following command in global configuration mode:

| Command | Purpose |
|-----------------------------|--|
| <code>rtr low-memory</code> | Specifies the amount of memory which must be available to allow SAA configuration. |

The **rtr low-memory** RTR configuration command allows you to specify the amount of memory that the SAA can use. The default value is 25 percent of the memory available on the system. If the amount of available free memory falls below the value specified in the **rtr low-memory** command, then the SAA will not allow new operations to be configured.

The value of the **rtr low-memory** command should not exceed the amount of free memory available on the system. To determine the amount of free memory available on the system, use the **show memory EXEC** command.

Configuring SAA Operations

Response time and availability information is collected by *operations* (formerly known as probes) that you configure on the router. 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.

SAA operations are given specific identification numbers so you can track the various operations you configure and execute. SAA operations are configured in RTR configuration mode. To configure an SAA operation, use the **rtr** global configuration command. When using this command, you specify the identification number for the operation you are about to configure. The router prompt will change to (`config-rtr`) to indicate that you are in RTR configuration mode.

To configure a new SAA operation, perform the following steps, beginning in global configuration mode:

-
- Step 1** Enter RTR configuration mode using the **rtr *op-number*** command. The *op-number* argument specifies an identification number for the operation you will be configuring.
 - Step 2** Use one of the **type** commands listed in the “Configuring the Operation Type” section which follows to specify which type of operation you are configuring.
 - Step 3** (Optional) Configure characteristics for the operation, one characteristic per line, using the commands found in “Configuring SAA Operation Characteristics” section on page 286.
 - Step 4** Type **exit** to return to global configuration mode.
 - Step 5** (Optional) Set reaction conditions for the operation, as explained in the “Reaction Thresholds” section on page 289.
 - Step 6** Schedule the operation start-time, as explained in the “Scheduling the Operation” section on page 290. For an example of this process, see the “IP/ICMP Path Echo Example” found in the “Examples” section.
-

Configuring the Operation Type

You must configure the operation type before you can configure any of the other characteristics. Cisco SA Agent currently allows the following types of operations:

| Operation Type | Function | RTR Configuration Command ¹ |
|---------------------|--|---|
| IP / ICMP Echo | The Internet Control Message Protocol (ICMP) Echo operation measures end-to-end response time between a Cisco router and devices using IP. ICMP is a network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Response time is computed by measuring the time taken between sending an ICMP echo request message to the destination and receiving an ICMP echo reply. Cisco SAA provides an option to compute response time on a specific path by using the Loose Source Routing option in IP packets. SAA also allows a user to measure Quality of Service (QoS) between endpoints by setting Type Of Service (TOS) bits on an IP packet. The Loose Source Routing path an IP/ICMP Echo operation should take can be set using the lsr-path command. | type echo protocol ipIcmpEcho |
| SNA Echo | The Systems Network Architecture (SNA) Echo operation measures end-to-end response time between a Cisco router and devices using SNA. You can use SNA's SSCP Native Echo (SSCP-RU), or you can target SNA LU type 0 connections or SNA LU type 2 connections which use Cisco's NSPECHO host application. | type echo protocol snaRUEcho or type echo protocol snaLU0EchoAppl or type echo protocol snaLU2EchoAppl |
| IP / ICMP Path Echo | Path Echo operations record statistics for each hop along the path that the operation takes to reach it destination. The ICMP Path Echo probe computes this hop-by-hop response time between a Cisco router and any IP device on the network by discovering the path using traceroute. Typical usage of this type of operation is to isolate bottlenecks in a path. Note Loose Source Routing (lsr) option is not available for this operation. | type pathEcho protocol IpIcmpEcho |
| TCP Connection | The Transmission Control Protocol (TCP) Connection operation is used to discover the time it takes to connect to the target device. This operation can be used to test virtual circuit availability or application availability. If the target is a Cisco router, then SA Agent makes a TCP connection to any port number specified by the user. If the destination is a non-Cisco IP host, then the user must specify a known target port number. This operation is useful in simulating Telnet or HTTP connection times. | type tcpConnect |

| Operation Type | Function | RTR Configuration Command ¹ |
|-------------------|---|--|
| UDP Echo | The User Datagram Protocol (UDP) Echo operation calculates UDP response times between a Cisco router and any IP enabled device. Response time is computed by measuring the time taken to send a datagram and receive a response from the destination device (round trip time). If the target is a Cisco router, then SAA sends a UDP datagram to any port number specified by the user. If the destination is a non-Cisco IP host, then the user must specify a known target port number. | type udpEcho |
| Jitter / UDP Plus | The UDP Plus operation is a superset of the UDP echo operation. In addition to measuring UDP round trip time, the UDP Plus operation measures per-direction packet-loss and Jitter. Jitter is inter-packet delay variance. Packet loss is a critical element in SLAs, and Jitter statistics are useful for analyzing traffic in a VoIP network. | type jitter |
| HTTP | <p>The HTTP operation measures the Round Trip Time (RTT) taken to connect and access data from an HTTP server. The HTTP server response time measurements consist of three types:</p> <ul style="list-style-type: none"> • DNS Lookup—RTT taken to perform domain name lookup. • TCP Connect—RTT taken to perform a TCP connect to the HTTP Server. • HTTP transaction time—RTT taken to send a request and get a response back from the HTTP Server (the probe retrieves the base HTML page only). <p>For a GET request, SAA will format the request based on the URL specified. In application self-service mode, the application controlling this probe is responsible for specifying the content of the HTTP request. SA Agent HTTP RAW operations allow the use of the http-raw-request Cisco IOS configuration submode. SAA will send the HTTP request, receive the reply, and report RTT statistics (including the size of the page returned).</p> | type http operation get or type http operation raw |
| DHCP | The SAA DHCP probe measures the round trip time taken to discover a DHCP Server and obtaining a lease from it. After obtaining an IP Address, SAA releases the IP address that was leased by the server. | type dhcp |

| Operation Type | Function | RTR Configuration Command ¹ |
|----------------|---|--|
| DLSw+ | <p>DLSw+ is the enhanced Cisco version of RFC 1795. DLSw+ tunnels LAN traffic over IP backbones via TCP. Many Enterprise customers use the DLSw+ technology to seamlessly connect LAN media over geographically disperse locations. The routers performing the tunneling of LAN traffic into TCP/IP are referred to as DLSw peers.</p> <p>The SAA DLSw+ probe measures the DLSw+ protocol stack and network response time between DLSw peers. Normally DLSw peers communicate through TCP port 2065. A prerequisite to successfully running the SAA DLSw+ probe is to have a connected DLSw+ peer between the source and destination Cisco devices. On the source DLSw+ device, a probe can be defined for a DLSw+ partner peer which doesn't have to be running a Cisco image which contains SA Agent functionality.</p> | type dlsw |
| DNS | <p>Domain Name System (DNS) response time is computed by taking the difference between the time taken to send DNS request and receiving a reply. The operation queries for an IP Address if the user specifies a host name or queries for a host name if the user specifies an IP Address.</p> | type dns |

1. For complete command syntax, use the ? (help) feature of the CLI, or refer to the Release 12.1 *Cisco IOS Configuration Fundamentals Command Reference*.

Support for FTP Get operations and One-way Delay operations is planned for Cisco IOS Release 12.1(1)T.

Configuring SAA Operation Characteristics

Characteristics you can configure for SAA operations are described in the following sections:

- Rate and Verification
- Statistics Information
- History
- Reaction Thresholds

Rate and Verification

To configure optional characteristics for Cisco SAA operations, use the following commands in RTR configuration mode:

| Command | Purpose |
|--|---|
| frequency <i>seconds</i> | Sets how often the operation should send a probe out to gather statistics. This command applies to all operation types. |
| lsr-path { <i>name</i> <i>ipaddr</i> } [<i>name</i> <i>ipaddr</i>] ... | Defines a Loose Source Routing (LSR) path for an IP/ICMP echo probe. This command applies only to IP/ICMP Echo operations (but not IP/ICMP Path Echo operations). |

| Command | Purpose |
|---------------------------------------|---|
| <code>owner text</code> | Configures the SNMP owner of the operation. This command applies to all operation types. |
| <code>request-data-size bytes</code> | Sets the protocol data size in the payload of the probe's request packet. This command applies to the following operation types: ICMP Echo, UPD Echo, Jitter, DLSW, and SNA Echo |
| <code>response-data-size bytes</code> | Sets the protocol data size in the payload of the probe's response packet. This command applies only to SNA Echo operations. |
| <code>tag text</code> | Logically links probes together in a group. This command applies to all operations. |
| <code>timeout milliseconds</code> | Sets the amount of time the probe waits for a response from its request packet. This command applies to all operations. |
| <code>threshold milliseconds</code> | Set the rising threshold (hysteresis) that generates a reaction event and stores history information for the operation. This command applies to all operations. |
| <code>tos number</code> | Defines the IP ToS byte for request packets. This command applies to the following operation types: ICMP Echo, UPD Echo, Jitter. |
| <code>verify-data</code> | Checks each operation response for corruption. This command applies to the following operation types: ICMP Echo and SNA Echo. |

Statistics Information

SAA operations capture statistics and collect error information. By default, the following information is captured and collected:

- Minimum and maximum response times
- Number of completions
- Sum of completion times
- Sum of the squares of completion times
- Accumulation of errors for noncompletions
- Total attempts (errors plus number of completions)
- Statistical distributions of response times

A statistical distribution of response times can be thought of as a set of buckets that holds the results of a probe. Each bucket holds the completion count that falls into that specific time interval. To modify the time intervals use the **statistics-distribution-interval** command. To modify the number of buckets use the **distributions-of-statistics-kept** command. For example, if the **statistics-distribution-interval** is 20 ms and the **distributions-of-statistics-kept** is 3 (buckets *a*, *b* and *c*) and 3 round-trip time (RTT) operations are performed with response times of 10 ms, 15 ms, and 30 ms, then the completion count for the buckets is 2 for *a*, 1 for *b*, and 0 for *c*.

In most situations, you do not need to change the statistical distribution interval or size. Only change the size when distributions are needed (for example, when performing statistical modeling of your network).

To control how much and what type of statistics are stored on the router, use the following optional commands in RTR configuration mode:

| Command | Purpose |
|---|---|
| <code>distributions-of-statistics-kept</code> <i>size</i> | Sets the number of buckets or statistical distributions kept during the probe's lifetime. Size is the number of buckets that contain data counts for their intervals. Applies to the following operations: ICMP Echo, ICMP PathEcho, UDP Echo, TcpConnect, DNS, DLSw, SNA Echo |
| <code>hops-of-statistics-kept</code> <i>size</i> | Collects pathEcho statistical distributions per hop per path. Size specifies the number of hops for which statistics are collected per path for each probe Applies to ICMP PathEcho operations only. |
| <code>hours-of-statistics-kept</code> <i>hours</i> | Sets the number of hours for which statistics are maintained for the probe. Applies to the following operations: ICMP Echo, ICMP PathEcho, UDP Echo, TcpConnect, DNS, DLSw, SNA Echo. For HTTP and Jitter operations, statistics are kept for the last two hours. This can not currently be reconfigured by a user. |
| <code>paths-of-statistics-kept</code> <i>size</i> | Collects statistical distributions for multiple paths. Size specifies the number of paths for which statistical distribution buckets are maintained per hour for each probe. Applies to ICMP PathEcho operations only. |
| <code>statistics-distribution-interval</code> <i>milliseconds</i> | Sets the time interval for each statistical distribution. Applies to the following operations: ICMP Echo, ICMP PathEcho, UDP Echo, TcpConnect, DNS, DLSw, SNA Echo. |



Note

When the **distribution-of-statistics-kept** command is set to default (1), you do not need to set the **statistics-distribution-interval** command because it has no effect on the statistics kept. For more information, refer to the command documentation in the “Router and Network Monitoring Commands” chapter of the Release 12.1 *Cisco IOS Configuration Fundamentals Command Reference*.

History

SAA can collect data samples for a given operation; these samples are called *history data*. By default, history data is not collected. When history collection is enabled, SAA collects the last *n* data points. The number of data points are configured using the **buckets-of-history-kept** command.

Additionally, when collecting history, SAA introduces the concept of *lives*. A life is defined as the operational lifetime of a probe. When a probe is stopped and restarted, data is kept in new life entries (if the number of entries is 2 or less). If the number of entries is more than 2, the oldest entry is overwritten by the new entry.

History is not supported for HTTP and Jitter operations.

**Note**

Collecting history increases the RAM usage. Collect history only when you think there is a problem in the network. For general network response time information, use the statistics collected by the SAA. Refer to the “Statistics Information” section for more information on statistics collection.

To control how much and what type of history is collected on the router, use the following commands in RTR configuration mode:

| Command | Purpose |
|---|--|
| <code>buckets-of-history-kept size</code> | For a pathEcho probe, sets the number of paths to store. For all other probes, sets the number (<i>size</i>) of data points to be kept. Applies to the following operations: ICMP Echo, ICMP PathEcho, UDP Echo, TcpConnect, DNS, DLSw, SNA Echo |
| <code>filter-for-history {none all overthreshold failures}</code> | Defines the type of information kept in the history table for the probe. This is a required command to enable history. All, overthreshold, or failures must be specified for history to work. Applies to the following operations: ICMP Echo, ICMP PathEcho, UDP Echo, TcpConnect, DNS, DLSw, SNA Echo. |
| <code>lives-of-history-kept lives</code> | Enables history collection and sets the number of lives maintained in the history table for the probe. Applies to the following operations: ICMP Echo, ICMP PathEcho, UDP Echo, TcpConnect, DNS, DLSw, SNA Echo |
| <code>samples-of-history-kept samples</code> | For a pathEcho probe, sets the number of hops in a path. For all other probes, RTR sets the number of samples to 1. Applies to the following operations: ICMP Echo, ICMP PathEcho, UDP Echo, TcpConnect, DNS, DLSw, SNA Echo |

To disable history collection, use the default value (0) for the **lives-of-history-kept** command rather than the **filter-for-history none** command. The **lives-of-history-kept** command disables history collection before the probe’s operation is attempted, and the **filter-for-history** command with the **none** keyword checks for history inclusion after the probe’s operation attempt is made.

Reaction Thresholds

You can configure the operation to send threshold notifications and use those notifications to trigger additional collection of time delay statistics. You can also configure the operation to send notifications when the probe loses connection, reestablishes connections, times out, and first succeeds after a timeout.

To configure the operation’s reaction conditions, use the following optional commands in global configuration mode:

| | Command | Purpose |
|--------|--|--|
| Step 1 | <code>rtr reaction-configuration number</code> <code>[connection-loss-enable] [timeout-enable]</code> <code>[threshold-falling milliseconds] [threshold-type option]</code> <code>[action-type option]</code> | Configures certain actions (for example, checking for connection losses or timeouts) to occur based on events controlled by the SAA. |
| Step 2 | <code>rtr reaction-trigger number target-number</code> | Defines an action-type which will activate the operation. |

Scheduling the Operation

After you have configured the operation, you must schedule the operation to begin capturing statistics and collecting error information. When scheduling an operation, it can start immediately or start at a certain month, day, or hour. The **pending** keyword is used when setting the operation to start at a later time. The **pending** keyword is also an internal state of the operation visible through SNMP. The pending state is also used when an operation is a reaction operation waiting to be triggered.

To schedule an SAA operation, use the following command in global configuration mode:

| Command | Purpose |
|---|---|
| <code>rtr schedule number [life seconds] [start-time {pending now hh:mm [month day day month]}] [ageout seconds]</code> | Schedules the operation by configuring the time parameters. |



Note

After you schedule the operation with the **rtr schedule** command, you cannot change the operation's configuration with the **rtr** global configuration command. To change the configuration of a scheduled operation, use the **no** form of the **rtr** command. The **no** form of the command removes all the operation's configuration information, including the schedule, reaction configuration, and reaction triggers. You can now create a new configuration for the operation.

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

Enabling the SAA Responder on Operational Targets

The SAA Responder is a feature which allows the use of UDP, Jitter, and TCP operations. The SA Agent Responder code must exist on target routers to support operations which probe non-native services such as the UDP echo operation and the TCP connection probe operation. Note that the Jitter operation is an enhanced UDP operation (UDP+). If UDP and TCP ports are chosen as targets for operations to which a router does not normally respond, the SA Agent Responder must be enabled to respond to SAA probe packets. If services that are already provided by the target router (such as Telnet or HTTP) are chosen, the SAA Responder does not need to be enabled. For non-Cisco devices, the SA Responder can not be configured and the SAA can send operational packets only to services native to those devices.

To enable SAA Responder functionality on a router, use the following command in global configuration mode:

| Command | Purpose |
|----------------------------|--|
| <code>rtr responder</code> | Enables SAA Responder functionality on a device. |

Configuring SAA Control Message Authentication

SAA uses a control message protocol to communicate with the Cisco routers that are the target of SAA operations. For security reasons, users have the option to enable authentication on the SAA Control Protocol. The authentication is provided using MD5 authentication. This authentication requires key definition on the source and target SAA routers. Configure the key using the **keychain** global configuration command to enter Keychain configuration mode.

For details on how to configure key chains, see the “Managing Authentication Keys” section in the “Configuring IP Routing Protocol-Independent Features” chapter of the *Cisco IOS IP and IP Routing Configuration Guide*. See also the “SAA Control Protocol Authentication Example” found in the Examples section below.

The **rtr key-chain** command notifies the SAA that it should use the previously configured key for authentication.

To configure the SAA RTR authentication, use the following command in global configuration mode:

| Command | Purpose |
|----------------------------------|--------------------------------------|
| rtr key-chain <i>name</i> | Configures SAA (RTR) authentication. |

Resetting the SAA

To perform an emergency reset of the SAA (including clearing all RTR configuration information), use the following command in global configuration mode:

| Command | Purpose |
|------------------|---|
| rtr reset | Stops all operations and clears all of the SAA RTR configuration information. |



Caution

Use the **rtr reset** command only in extreme situations such as the incorrect configuration of a number of operations. The **rtr reset** command reconfigures the router to its startup configuration.

In addition to stopping all operations and clearing the RTR configuration information, the **rtr reset** command returns the SAA to the startup condition. This command does not reread the configuration stored in NVRAM. You must retype the SAA’s configuration or use the **config memory** command (this has the side effect of reconfiguring the router to its startup configuration).

Viewing SAA Operational Results and SAA Status

To display information about the status and configuration of the SAA, use the following commands in EXEC mode. You can display information in a tabular or full format. Tabular format displays information in a column reducing the number of screens required to display the information. Full format displays all information using identifiers next to each displayed value.

| Command | Purpose |
|--|---|
| <code>show rtr application [tabular full]</code> | Displays global information about the RTR feature. |
| <code>show rtr authentication</code> | Displays authentication information. |
| <code>show rtr collection-statistics [number] [tabular full]</code> | Displays error totals collected for all operations or a specified operation. |
| <code>show rtr configuration [number] [tabular full]</code> | Displays configuration values including all defaults for all operations or a specified operation. |
| <code>show rtr distributions-statistics [number] [tabular full]</code> | Displays statistical distribution information (captured response times) for all operations or a specified operation. |
| <code>show rtr history [number] [tabular full]</code> | Displays history collected for all operations or a specified operation. |
| <code>show rtr operational-state [number] [tabular full]</code> | Displays the operational state of all operations or a specified operation. |
| <code>show rtr reaction-trigger [number] [tabular full]</code> | Displays the reaction trigger information for all operations or a specified operation. |
| <code>show rtr responder</code> | Displays responder information. |
| <code>show rtr totals-statistics [number] [tabular full]</code> | Displays the total statistic values (accumulation of error counts and completions) for all operations or a specified operation. |

SAA Configuration Examples

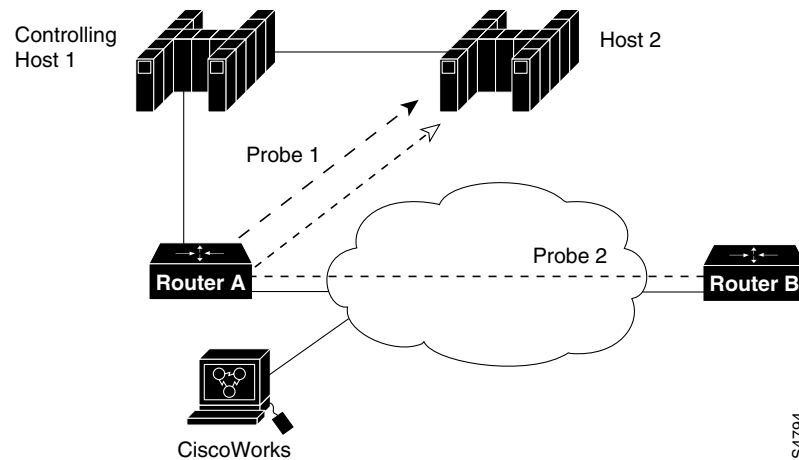
This section provides the following configuration examples for setting up operations on the router to monitor network performance and send notifications:

- SNA Echo Example
- IP/ICMP Path Echo Example
- TcpConnect Example
- SAA Control Protocol Authentication Example
- Jitter Operation Example
- HTTP GET Operation Example
- HTTP RAW operation using RAW submode
- HTTP RAW operation through a Proxy Server
- DNS Operation Example
- DLSw Operation Example
- DHCP Operation Example
- Connection Loss Trigger Example

SNA Echo Example

The example in Figure 22 shows probe 1 configured from Router A to Host 2, and Probe 2 is configured from Router B to Host 2. This configuration allows normative analysis of the network to determine a baseline from which triggers (and general reactions) are configured. Also, two SNA PUs must be configured: CWBC0A and CWBC0B. For information on configuring SNA PUs, see the **dspu host** or the **sna host** commands in the *Cisco IOS Bridging and IBM Networking Command Reference*.

Figure 22 Configure Probes for Normative Analysis—SNA LU2



Configuration for Router A

```
RouterA(config)# rtr 1
RouterA(config-rtr)# type echo protocol snaLU2EchoAppl CWBC0A
RouterA(config-rtr)# exit
RouterA(config)# rtr schedule 1 start-time now
RouterA(config)# exit
```

Configuration for Router B

```
RouterB(config)# rtr 2
RouterB(config-rtr)# type echo protocol snaLU2EchoAppl CWBC0B
RouterB(config-rtr)# exit
RouterB(config)# rtr schedule 1 start-time now
RouterB(config)# exit
```

Configuration Files for Router A and Router B

After you save the configurations for Router A and Router B (using the **copy running-config startup-config** command), information is stored in the configuration files. The following information is stored:

```
!Router A Configuration File
! Router A's PU Configuration
sna host CWBC0A xid-snd 05dcc00a rmac 4001.3745.1088 rsap 4 lsap 12 focalpoint
rtr 1
  type echo protocol snaLU2EchoAppl CWBC0A
  paths-of-statistics-kept 1
  hops-of-statistics-kept 1
  samples-of-history-kept 1
rtr schedule 1 start-time now
```

```

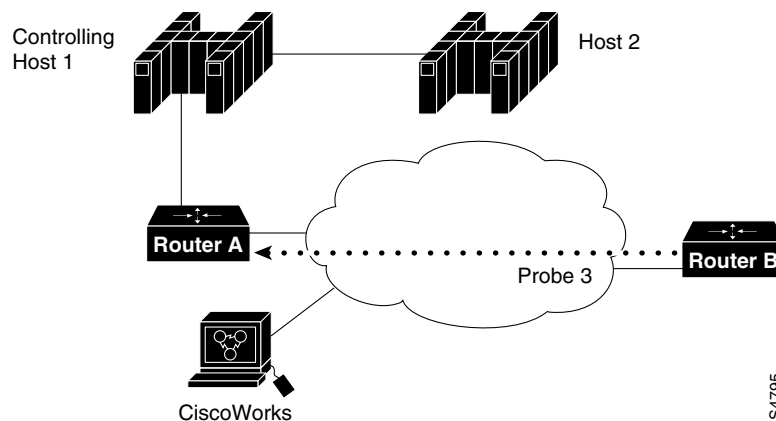
!Router B Configuration File
!Router B's PU Configuration from the Configuration File:
sna host CWBC0B xid-snd 05dcc00b rmac 4001.3745.1088 rsap 4 lsap 12 focalpoint
rtr 2
  type echo protocol snaLU2EchoAppl CWBC0B
  paths-of-statistics-kept 1
  hops-of-statistics-kept 1
  samples-of-history-kept 1
rtr schedule 2 start-time now

```

IP/ICMP Path Echo Example

The example in Figure 23 shows that Probe 3 is configured from Router B to Router A to perform network troubleshooting and identify network problems that configure triggers and general reactions.

Figure 23 Configure a Probe for Troubleshooting—IP/ICMP



This example sets up a pathEcho (with history) pending entry from Router B to Router A via IP/ICMP. It attempts to execute 3 times in 25 seconds (first attempt starts at 0 seconds) and keeps those 3 times with 3 buckets. The entry can be started 5 times before wrapping over stored history (**lives-of-history-kept** = 5). Because this configuration keeps history, it uses more RAM on the router.

Configuration for Router B

```

RouterB(config)# rtr 3
RouterB(config-rtr)# type pathEcho protocol ipIcmpEcho RouterA
RouterB(config-rtr)# frequency 10
RouterB(config-rtr)# lives-of-history-kept 5
RouterB(config-rtr)# buckets-of-history-kept 3
RouterB(config-rtr)# filter-for-history all
RouterB(config-rtr)# exit
RouterB(config)# rtr schedule 3 life 25
RouterB(config)# exit

```

Configuration File for Router B

After you save the configuration (using the **copy running-config startup-config** command) the information is stored in the configuration file. Note the addition of the response-data-size command in the configuration file. Some necessary default forms of commands are automatically included if they are not specified in the configuration setting, based on their necessity for operation execution. The following information is stored:

```

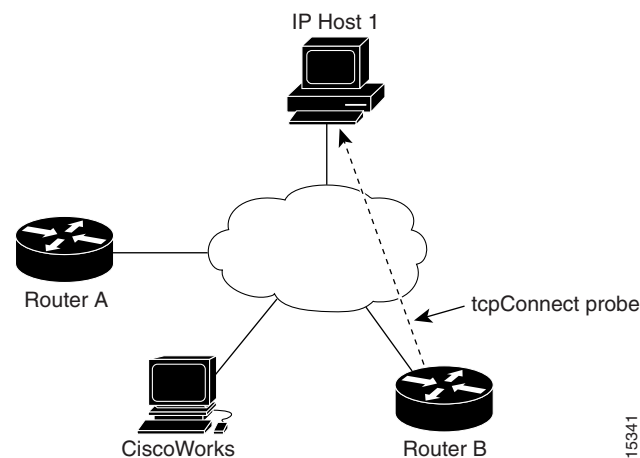
rtr 3
type pathEcho protocol ipIcmpEcho 172.28.161.21
frequency 10
response-data-size 1
lives-of-history-kept 5
buckets-of-history-kept 3
filter-for-history all
rtr schedule 3 life 25 start-time pending

```

TcpConnect Example

The example in Figure 24 shows a tcpConnect probe configured from Router B to the Telnet port (TCP port 23) of IP Host 1 (IP address 10.0.0.1).

Figure 24 Configuring a tcpConnect Probe



Configuration for Router B

```

RouterB(config)# rtr 5
RouterB(config-rtr)# type tcpConn dest-ipaddr 10.0.0.1 dest-port 23 control disable
RouterB(config-rtr)# exit
RouterB(config)# rtr schedule 5 start now

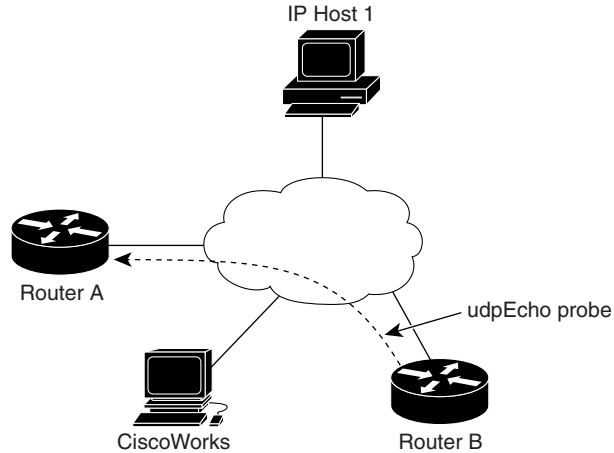
```

In the example the control protocol for the probe is disabled. RTR collector uses the RTR control protocol to notify the SAA Responder on the responder router to enable the target port temporarily. This action allows the responder to respond to the probe packet. In this case, because the target is not a router and a well known TCP port is used, there is no need to send the control message.

SAA Control Protocol Authentication Example

The example in Figure 25 shows a udpEcho probe configured from Router B to UDP port 888 on Router A (IP address 20.0.0.1).

Figure 25 Configuring a udpEcho Probe



15342

**Note**

Configuring SAA control protocol authentication is optional. However, if you configure authentication for Router B, you must configure the same authentication for Router A.

In the following configuration example, a keychain called “csaa-key” is configured on both routers. The **rtr key-chain** command enables RTR MD5 authentication on the control messages.

Configuration for Router A

```
RouterA(config)# key chain csaa-key
RouterA(config-keychain)# key 1
RouterA(config-keychain-key)# key-string secret
RouterA(config-keychain-key)# exit
RouterA(config-keychain)# exit
RouterA(config)# rtr key-chain csaa-key
RouterA(config)# rtr responder
```

Configuration for Router B

```
RouterB(config)# key chain csaa-key
RouterB(config-keychain)# key 1
RouterB(config-keychain-key)# key-string secret
RouterB(config-keychain-key)# exit
RouterB(config-keychain)# exit
RouterB(config)# rtr key-chain csaa-key
RouterB(config)# rtr 6
RouterB(config-rtr)# type udpEcho dest-ipaddr 20.0.0.1 dest-port 888 control enable
RouterB(config-rtr)# exit
RouterB(config)# rtr schedule 6 start now
```

Jitter Operation Example

In order to perform an Jitter operation (also known as a UDP+ operation), SAA Responder must be enabled on the target router using the **rtr responder** command.

**Note**

Use the **rtr responder** command with the **type udpEcho** keyword combination for Jitter (UDP Echo+) operations.

A Jitter operation consists of a train of packets sent at a constant interval. The numbers of packets sent and the interval are user-configurable. When the SAA Responder receives the packets, it timestamps the reception time and then sends the packet back.

Based on timestamps from consecutive packets, the sender can calculate the jitter value, which is the difference in the latency. Specifically, the jitter is computed as follows:

For 2 packets, packet #1 (P1) and packet#2 (P2),
the Jitter between P1 and P2 is

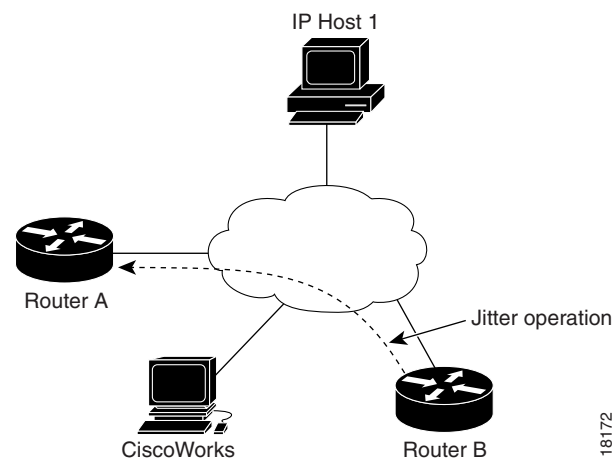
$$(R2 - S2) - (R1 - S1) == (R2 - R1) - (S2 - S1),$$

where S1 is the sending time for P1 on the source; R1 is the receiving time for P1 on the target; S2 is the sending time for P2; and R2 is the receiving time for P2.

Note that the clocks on the two devices do not need to be synchronized.

In the example shown in Figure 26, SAA operation number 200 is created and configured as a Jitter (UDP+) operation using the destination IP address 172.24.132.100, destination UDP port number 99. The operation will send 20 packets at 20 ms intervals.

Figure 26 Jitter Operation



Configuration for Router A

The SAA Responder must be enabled on Router A for the Jitter operation to run.

```
RouterA(config)# rtr responder type udpEcho ipaddr 172.24.132.100 port 99
```

Configuration for Router B

```
RouterB(config)#rtr 200
RouterB(config-rtr)#type jitter dest-ip 172.24.132.100 dest-port 99 num-packets 20
interval 20
```

After the Jitter operation has run, you can view the results with the **show rtr collection statistics** command. The following example shows sample output:

```
Entry Number: 200
Target Address: 172.24.132.100, Port Number: 31337
Start Time: *14:14:14.000 EST Thu Apr 6 2000
RTT Values:
NumOfRTT: 2800 RTTSum: 4792 RTTSum2: 8830
Packet Loss Values:
```

```

PacketLossSD: 0 PacketLossDS: 0
PacketOutOfSequence: 0 PacketMIA: 0 PacketLateArrival: 0
InternalError: 0 Busies: 0
Jitter Values:
MinOfPositivesSD: 1 MaxOfPositivesSD: 1
NumOfPositivesSD: 249 SumOfPositivesSD: 249 Sum2PositivesSD: 249
MinOfNegativesSD: 1 MaxOfNegativesSD: 2
NumOfNegativesSD: 238 SumOfNegativesSD: 239 Sum2NegativesSD: 241
MinOfPositivesDS: 1 MaxOfPositivesDS: 1
NumOfPositivesDS: 97 SumOfPositivesDS: 97 Sum2PositivesDS: 97
MinOfNegativesDS: 1 MaxOfNegativesDS: 1
NumOfNegativesDS: 92 SumOfNegativesDS: 92 Sum2NegativesDS: 92

```

The values shown indicate the aggregated values for the current hour. RTT stands for Round-Trip-Time. SD stands for Source-to-Destination. DS stands for Destination-to-Source. Table 19 describes the significant fields shown in this output.

Table 19 *show rtr collection-statistics Field Descriptions*

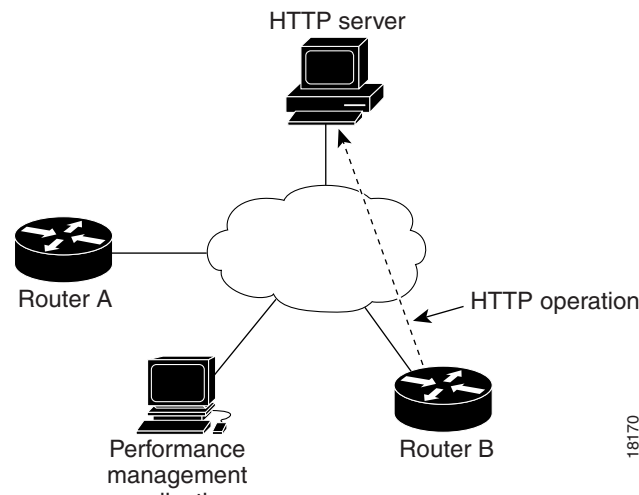
| Field | Description |
|--------------------------------------|--|
| NumOfRTT | The number of successful round trips. |
| RTTSum | The sum of those round trip values (in milliseconds). |
| RTTSum2 | The sum of squares of those round trip values (in milliseconds). |
| PacketLossSD | The number of packets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

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

HTTP GET Operation Example

In the example shown in Figure 27, operation 5 is created and configured as an HTTP GET operation. The destination URL is `http://www.cisco.com`:

Figure 27 HTTP Operation



Configuration for Router B

```
RouterB(config)#rtr 5
RouterB(config-rtr)#type http operation get url http://www.cisco.com
RouterB(config-rtr)# exit
RouterB(config)# rtr schedule 5 start-time now
```

HTTP RAW operation using RAW submode

In the following example, SAA operation 6 is created and configured as an HTTP RAW operation. To use the raw commands, HTTP-RAW submode is entered using the `http-raw-request` command. The RTR HTTP-RAW configuration submode is indicated by the `(config-rtr-http)` router prompt.

```
(config)# rtr 6
(config-rtr)# type http operation raw url http://www.cisco.com
(config-rtr)# http-raw-request
(config-rtr-http)# GET /index.html HTTP/1.0\r\n
(config-rtr-http)# \r\n
(config-rtr-http)# exit
(config)# rtr schedule 6 start-time now
```

HTTP RAW operation through a Proxy Server

In this example `http://www.proxy.cisco.com` is the proxy server and `http://www.xyz.com` is the HTTP Server.

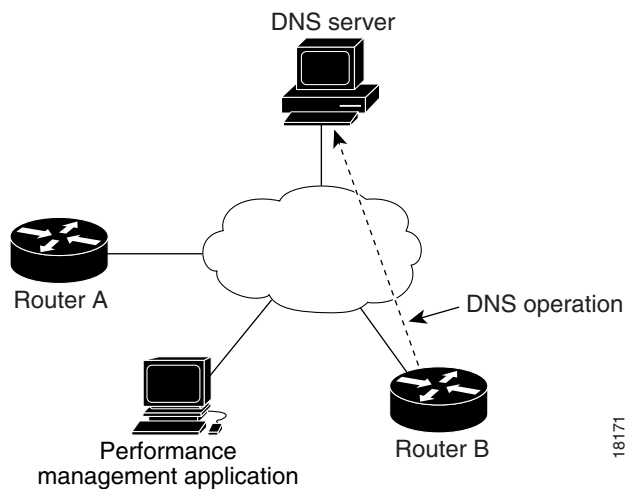
```
(config)# rtr 6
```

```
(config-rtr)# type http operation raw url http://www.proxy.cisco.com
(config-rtr)# http-raw-request
(config-rtr-http)# GET http://www.xyz.com HTTP/1.0\r\n
(config-rtr-http)# \r\n
(config-rtr-http)# exit
(config)# rtr schedule 6 start-time now
```

DNS Operation Example

In the example shown in Figure 28, SAA operation 7 is created and configured as a DNS operation using the name server IP address 172.20.2.132:

Figure 28 DNS Operation

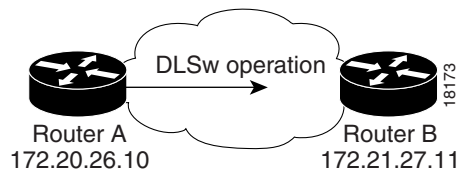


```
RouterB(config)#rtr 7
RouterB(config-rtr)#type dns target-addr lethe name-server 172.20.2.132
```

DLSw Operation Example

In the example shown in Figure 29, DLSw peers 172.20.26.10 and 172.21.27.11 are configured:

Figure 29 DLSw Operation



```
!Configuration excerpt from Router A
dlsw local-peer peer-id 172.20.26.10
dlsw remote-peer 0 tcp 172.21.27.11
rtr 1
type dlsw peer-ipaddr 172.21.27.11
rtr schedule 1 start-time now
```

```
!Configuartion excerpt from Router B
```

```
dlsw local-peer peer-ip 172.21.27.11
dlsw remote-peer 0 tcp 172.20.26.10
```

DHCP Operation Example

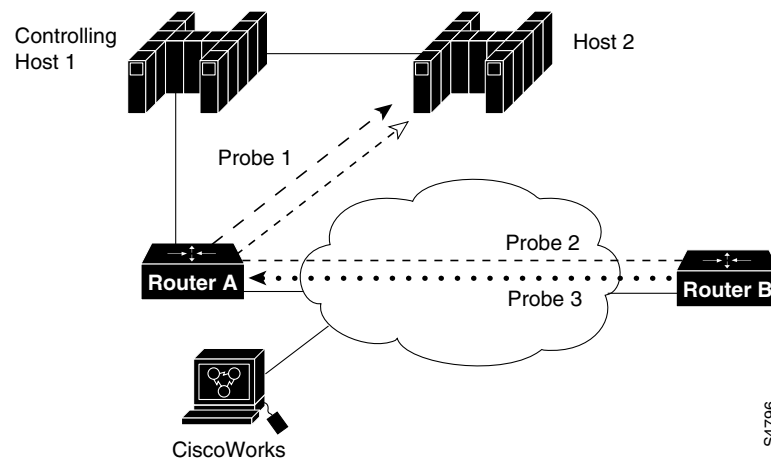
In the following example, SAA operation number 4 is configured as a DHCP operation enabled for DHCP server 172.16.20.3:

```
(config)# rtr 4
(config-rtr)# type dhcp
(config)# ip dhcp-server 172.16.20.3
```

Connection Loss Trigger Example

Figure 30 shows SAA operations (probes) 1, 2, and 3 in the network. This example shows how to configure a trigger if Probe 2 encounters a connection loss from Router B to Host 2. If a connection loss occurs between Router B and Host 2, a trap is issued, an SNA NMVT Alert is issued, and the Probe 3 state is changed to active.

Figure 30 Configure a Trigger for Connection Loss



Router B Configuration

```
RouterB(config)# rtr reaction-configuration 2 connection-loss-enable
                 action-type trapNmvtAndTrigger
RouterB(config)# rtr reaction-trigger 2 3
```



Note

The operation numbers must be unique within only one router. The examples shown use three different probe operation numbers for clarity.

