



Configuring Cisco IP SLAs UDP Jitter Operation

Cisco IP Service Level Agreements (IP SLAs) functionality is embedded in most devices that run Cisco IOS software, which allow Cisco customers to analyze IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce the frequency of network outages. IP SLAs use active traffic monitoring—the generation of traffic in a continuous, reliable, and predictable manner—for measuring network performance. Using IP SLAs, service provider customers can measure and provide service level agreements, and enterprise customers can verify service levels, verify outsourced service level agreements, and understand network performance. IP SLAs can perform network assessments, verify quality of service (QoS), ease the deployment of new services, and assist administrators with network troubleshooting. IP SLAs can be accessed using the Cisco IOS command-line interface (CLI) or Simple Network Management Protocol (SNMP) (through the Cisco Round-Trip Time Monitor [RTTMON] and SYSLOG Management Information Bases [MIBs]).

This document describes Cisco's cross-platform IP SLAs functionality. However, the Catalyst 3750 Metro switch and the Cisco ME 3400 switch platforms have been tested only in this limited configuration:

1. Two switches connected back-to-back.
2. No protocols running on the switch CPUs, including STP.
3. Jitter probe send and receive rate:
 - a. 50 bidirectional probes sent with each probe consisting of up to 50 packets sent at 1-second intervals.
 - b. Probes started with a 1-second stagger between each probe.

Additional IP SLAs commands and configuration options have not been tested on these platforms and are not supported.

The Catalyst 3750 Metro and Cisco ME 3400 switches can initiate and reply to jitter probes. However, the traffic does not follow the queuing configuration that is applied to customer traffic. All locally originated traffic always goes to the same egress queue on the switch port, regardless of the ToS setting for the IP SLAs probe. We recommend the use of an external shadow router to measure latency and packet drop rate (PDR) across the switch.

Contents

- [Cisco IOS IP SLAs Overview, page 2](#)
- [Analyzing IP Service Levels Using the IP SLAs UDP Jitter Operation, page 9](#)
- [Command Reference, page 26](#)
- [Obtaining Documentation, page 34](#)
- [Documentation Feedback, page 35](#)
- [Cisco Product Security Overview, page 35](#)
- [Obtaining Technical Assistance, page 36](#)
- [Obtaining Additional Publications and Information, page 37](#)

Cisco IOS IP SLAs Overview

This overview includes these sections:

- [Prerequisites for Cisco IOS IP SLAs, page 2](#)
- [Information About Cisco IOS IP SLAs, page 2](#)
- [Information About the IP SLAs UDP Jitter Operation, page 9](#)
- [How to Configure the IP SLAs UDP Jitter Operation, page 10](#)
- [Configuration Example for the IP SLAs UDP Jitter Operation, page 25](#)

Prerequisites for Cisco IOS IP SLAs

Knowledge of general networking protocols and your specific network design is assumed. Familiarity with network management applications is useful.

Information About Cisco IOS IP SLAs

To implement general configuration and scheduling of IP SLAs, you should understand the following concepts:

- [Cisco IOS IP SLAs Technology Overview, page 3](#)
- [Service Level Agreements, page 4](#)
- [Benefits of IP SLAs, page 5](#)
- [Network Performance Measurement Using IP SLAs, page 5](#)
- [IP SLAs Responder and IP SLAs Control Protocol, page 6](#)
- [Response Time Computation for IP SLAs, page 7](#)
- [IP SLAs Operation Scheduling, page 8](#)

Cisco IOS IP SLAs Technology Overview

IP SLAs use active traffic monitoring—the generation of traffic in a continuous, reliable, and predictable manner—for measuring network performance. Cisco IOS IP SLAs send data across the network to measure performance between multiple network locations or across multiple network paths. They simulate network data and IP services, and collect network performance information in real time. The information collected includes data about response time, one-way latency, jitter (interpacket delay variance), packet loss, voice quality scoring, network resource availability, application performance, and server response time. IP SLAs originated from the technology previously known as Service Assurance Agent (SAA). IP SLAs perform active monitoring by generating and analyzing traffic to measure performance either between Cisco IOS devices or from a Cisco IOS device to a remote IP device such as a network application server. Measurement statistics provided by the various IP SLAs operations can be used for troubleshooting, for problem analysis, and for designing network topologies.

Using IP SLAs, service provider customers can measure and provide service level agreements, and enterprise customers can verify service levels, verify outsourced service level agreements, and understand network performance for new or existing IP services and applications. IP SLAs use unique service level assurance metrics and methodology to provide highly accurate, precise service level assurance measurements.

Being Layer-2 transport independent, IP SLAs can be configured end-to-end over disparate networks to best reflect the metrics that an end-user is likely to experience. IP SLAs collect a unique subset of the following performance metrics:

- Delay (both round-trip and one-way)
- Jitter (directional)
- Packet loss (directional)
- Packet sequencing (packet ordering)
- Path (per hop)
- Connectivity (directional)
- Server or website download time
- Voice quality scores

Because IP SLAs are accessible using SNMP, they also can be used by performance monitoring applications like CiscoWorks Internetwork Performance Monitor (IPM) and other third-party Cisco partner performance management products. More details about network management products that use IP SLAs can be found at the following URL:

<http://www.cisco.com/go/ipsla>

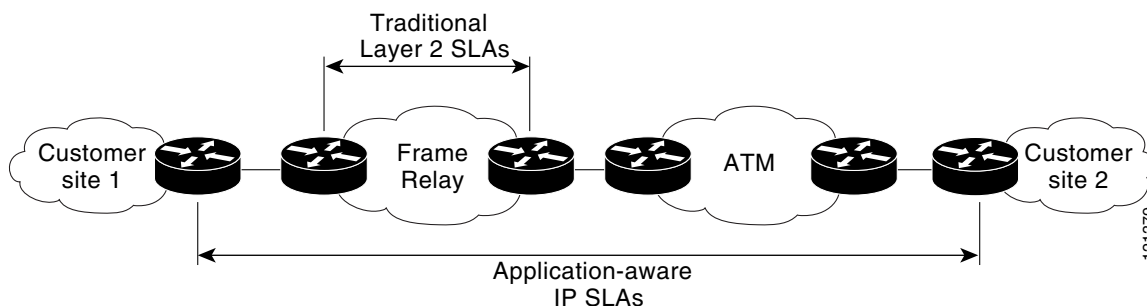
SNMP notifications based on the data gathered by an IP SLAs operation allow the router to receive alerts when performance drops below a specified level and when problems are corrected. IP SLAs use the Cisco RTTMON MIB for interaction between external Network Management System (NMS) applications and the IP SLAs operations running on the Cisco devices. For a complete description of the object variables referenced by the IP SLAs feature, refer to the text of the CISCO-RTTMON-MIB.my file, available from the Cisco MIB website.

Service Level Agreements

Internet commerce has grown significantly in the past few years as the technology has advanced to provide faster, more reliable access to the Internet. Many companies now need online access and conduct most of their business online and any loss of service can affect the profitability of the company. Internet service providers (ISPs) and even internal IT departments now offer a defined level of service—a service level agreement—to provide their customers with a degree of predictability.

The latest performance requirements for business-critical applications, voice over IP (VoIP) networks, audio and visual conferencing, and VPNs are creating internal pressures on converged IP networks to become optimized for performance levels. Network administrators are increasingly required to support service level agreements that support application solutions. Figure 1 shows how IP SLAs have taken the traditional concept of Layer 2 service level agreements and applied a broader scope to support end-to-end performance measurement, including support of applications.

Figure 1 Scope of Traditional Service Level Agreement Versus Cisco IOS IP SLAs



IP SLAs provide the following improvements over a traditional service level agreement:

- End-to-end measurements—The ability to measure performance from one end of the network to the other allows a broader reach and more accurate representation of the end-user experience.
- Sophistication—Statistics such as delay, jitter, packet sequence, Layer 3 connectivity, and path and download time that are broken down into bidirectional and round-trip numbers provide more data than just the bandwidth of a Layer 2 link.
- Accuracy—Applications that are sensitive to slight changes in network performance require the precision of the sub-millisecond measurement of IP SLAs.
- Ease of deployment—Leveraging the existing Cisco devices in a large network makes IP SLAs easier and cheaper to implement than the physical probes often required with traditional service level agreements.
- Application-aware monitoring—IP SLAs can simulate and measure performance statistics generated by applications running over Layer 3 through Layer 7. Traditional service level agreements can only measure Layer 2 performance.
- Pervasiveness—IP SLAs support exists in Cisco networking devices ranging from low-end to high-end routers and switches. This wide range of deployment gives IP SLAs more flexibility over traditional service level agreements.

When you know the performance expectations for different levels of traffic from the core of your network to the edge of your network, you can confidently build an end-to-end application-aware service level agreement.

Benefits of IP SLAs

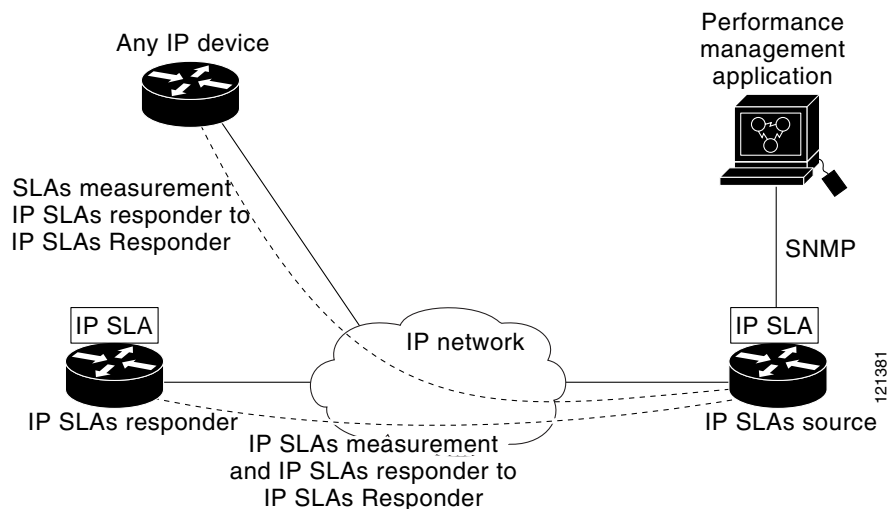
- IP SLAs monitoring— Provides service level agreement monitoring, measurement, and verification.
- Network performance monitoring
 - Measures the jitter, latency, or packet loss in the network.
 - Provides continuous, reliable, and predictable measurements.
- IP service network health assessment—Verifies that the existing QoS is sufficient for new IP services.
- Edge-to-edge network availability monitoring—Provides proactive verification and connectivity testing of network resources (for example, indicates the network availability of an NFS server used to store business critical data from a remote site).
- Troubleshooting of network operation—Provides consistent, reliable measurement that immediately identifies problems and saves troubleshooting time.

Network Performance Measurement Using IP SLAs

IP SLAs functionality is embedded in Cisco IOS software and it is included in all the networking devices that run Cisco IOS software. A network engineer can monitor the performance between any area in the network: core, distribution, and edge. Monitoring can be done anytime, anywhere, without deploying a physical probe.

IP SLAs use generated traffic to measure network performance between two networking devices such as routers. [Figure 2](#) shows how IP SLAs start when the IP SLAs device sends a generated packet to the destination device. After the destination device receives the packet, and depending on the type of IP SLAs operation, the device will respond with time-stamp information for the source to make the calculation on performance metrics. An IP SLAs operation is a network measurement to a destination in the network from the source device using a specific protocol such as UDP for the operation.

Figure 2 IP SLAs Operations



There are three main types of IP SLAs operations:

- Responder-based
- Internet Control Message Protocol (ICMP)
- Nonresponder-based

In responder-based operations the IP SLAs Responder is enabled in the destination device and provides information such as the processing delays of IP SLAs packets. The responder-based operation has improved accuracy over the ICMP operation discussed above, and offers the capability of unidirectional measurements. In replies to the IP SLs source device, the responder includes information about processing delays. The IP SLAs source device can then remove the delays in its final performance calculation. Use of the responder is optional for the UDP Echo operation, and the TCP Connect operation, but it is required for the UDP Jitter operation.

In ICMP operations, the source IP SLAs device sends several ICMP packets to the destination. The destination device—any IP device—echoes with replies. The source IP SLAs device uses the sent and received time stamps to calculate the response time. The ICMP Echo operation resembles the traditional extended ping utility, and it measures only the response time between the source device and the destination device. ICMP Path Echo and Path Jitter operations use the traceroute utility to identify the whole path. Subsequent ICMP packets are sent to each path node and the measurements are correlated to provide hop-by-hop round-trip delay and also jitter information.

Nonresponder-based operations are used to monitor specific traffic types such as HTTP, FTP, DHCP, and TCP Connect. The destination device can be any IP device that supports the protocol being monitored. The measurement metrics vary from protocol to protocol. The most important measurement is usually the server response time because the destination device acts as the server for the protocol.

To implement IP SLAs network performance measurement, you need to perform these tasks:

1. Enable the IP SLAs Responder, if appropriate.
2. Configure the required IP SLAs operation type.
3. Configure any options available for the specified IP SLAs operation type.
4. Configure threshold conditions, if required.
5. Schedule the operation to run, then let the operation run for a period of time to gather statistics.
6. Display and interpret the results of the operation using Cisco IOS CLI or an NMS system with SNMP.

This section includes conceptual information about the IP SLAs Responder and IP SLAs control protocol, response time, and scheduling options.

For configuration information about IP SLAs UDP operation, see the [“Analyzing IP Service Levels Using the IP SLAs UDP Jitter Operation”](#) section on page 9.

IP SLAs Responder and IP SLAs Control Protocol

The IP SLAs Responder is a component embedded in the destination Cisco routing device that allows the system to anticipate and respond to IP SLAs request packets. IP SLAs Responder provides an enormous advantage with accurate measurements without the need for dedicated probes and additional statistics not available via standard ICMP-based measurements. The patented IP SLAs Control Protocol is used by the IP SLAs Responder providing a mechanism through which the responder can be notified on which port it should listen and respond. Only a Cisco IOS device can be a source for a destination IP SLAs Responder.

Figure 2 shows where the IP SLAs Responder fits in relation to the IP network. The IP SLAs Responder listens on a specific port for control protocol messages sent by IP SLAs. Upon receipt of the control message, the responder will enable the specified UDP or TCP port for the specified duration. During this time, the responder accepts the requests and responds to them. The responder disables the port after it responds to the IP SLAs packet, or when the specified time expires. For added security, MD5 authentication for control messages is available.

The IP SLAs Responder must be used with the UDP Jitter operation, but it is optional for UDP Echo and TCP Connect operations. If services that are already provided by the target router (such as Telnet or HTTP) are chosen, the IP SLAs Responder need not be enabled. For non-Cisco devices, the IP SLAs Responder cannot be configured and the IP SLAs can send operational packets only to services native to those devices.

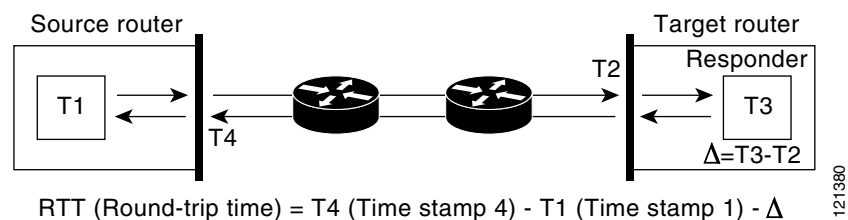
Response Time Computation for IP SLAs

Routers may take tens of milliseconds to process incoming packets, due to other high priority processes. This delay affects the response times because the reply to test packets might be sitting on queue while waiting to be processed. In this situation, the response times would not accurately represent true network delays. Cisco IOS IP SLAs minimize these processing delays on the source router as well as on the target router (if Cisco IOS IP SLAs Responder is being used), in order to determine true round-trip times. IP SLAs test packets use time stamping to minimize the processing delays.

When enabled, the IP SLAs Responder allows the target device to take two time stamps both when the packet arrives on the interface at interrupt level and again just as it is leaving, eliminating the processing time. This time stamping is made with a granularity of sub-millisecond (ms). At times of high network activity, an ICMP ping test often shows a long and inaccurate response time, while an IP SLAs test shows an accurate response time due to the time stamping on the responder.

Figure 3 demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target router, with the responder functionality enabled time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source router where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy.

Figure 3 IP SLAs Responder Time Stamping



An additional benefit of the two time stamps at the target router is the ability to track one-way delay, jitter, and directional packet loss. Because much network behavior is asynchronous, it is critical to have these statistics. However, to capture one-way delay measurements the configuration of both the source router and target router with Network Time Protocol (NTP) is required. Both the source and target need to be synchronized to the same clock source. One-way jitter measurements do not require clock synchronization.

IP SLAs Operation Scheduling

After an IP SLAs operation has been configured, 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, and hour. There is a pending option to set the operation to start at a later time. The pending option is also an internal state of the operation visible through SNMP. The pending state is also used when an operation is a reaction (threshold) operation waiting to be triggered. Normal scheduling of IP SLAs operations allows you to schedule one operation at a time.

Multiple operations scheduling allows you to schedule multiple IP SLAs operations using a single command through the Cisco IOS CLI or the CISCO RTTMON-MIB. This feature allows you to control the amount of IP SLAs monitoring traffic by scheduling the operations to run at evenly distributed times. This distribution of IP SLAs operations helps minimize the CPU utilization and thereby enhances the scalability of the network. You must specify the operation ID numbers to be scheduled and the time range over which all the IP SLAs operations should start. This feature automatically distributes the IP SLAs operations at equal intervals over a specified time frame. The spacing between the operations (start interval) is calculated and the operations are started.

The IP SLAs multiple operations scheduling functionality allows you to schedule multiple IP SLAs operations as a group using the **rtr group schedule** command. The following parameters can be configured with this command:

Group operation number—Group configuration or group schedule number of the IP SLAs operation to be scheduled.

Operation ID numbers—A list of IP SLAs operation ID numbers in the scheduled operation group.

Schedule period—Amount of time for which the IP SLAs operation group is scheduled.

Ageout—Amount of time to keep the operation in memory when it is not actively collecting information. By default, the operation remains in memory indefinitely.

Frequency—Amount of time after which each IP SLAs operation is restarted.

Life—Amount of time the operation actively collects information. The operation can be configured to run indefinitely. By default, the lifetime of an operation is one hour.

Start time—Time when the operation starts collecting information. You can specify an operation to start immediately or at an absolute start time using hours, minutes, seconds, day, and month.



Note

The scheduling of multiple IP SLAs operations does not support the recurring functionality.

The IP SLAs multiple operations scheduling functionality schedules the maximum number of operations possible without aborting. The total number of operations will be calculated based on the number of operations specified in the command, irrespective of the number of operations that are missing—operations that are scheduled, but are not configured—or already running. If you schedule operations that are not configured or are already running, IP SLAs display a message showing the number of active and missing operations.

A main benefit for scheduling multiple IP SLAs operations is to distribute the operations equally over a scheduled period, which helps you achieve more consistent monitoring coverage. To illustrate this scenario, consider configuring 60 operations to start during the same 1-second interval over a 60-second schedule period. If a network failure occurs 30 seconds after all 60 operations have started and the network is restored before the operations are due to start again (in another 30 seconds), then this failure would never be detected by any of the 60 operations. However, if the 60 operations are distributed equally at 1-second intervals over a 60-second schedule period, then some of the operations would detect the network failure.

Operations of the same type and same frequency should be used for IP SLAs multiple operations scheduling. If you do not specify a frequency, the default frequency will be the same as that of the schedule period. The schedule period is the period of time in which all the specified operations should run.

When you reboot the router, the IP SLAs multiple operations scheduling functionality is not affected.

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> CISCO-RTTMON-MIB; “Response Time Monitor MIB” 	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

Analyzing IP Service Levels Using the IP SLAs UDP Jitter Operation

This section describes how to use the Cisco IOS IP SLAs UDP Jitter operation to analyze round-trip delay, one-way delay, one-way jitter, one-way packet loss, and connectivity in networks that carry UDP traffic.

Cisco IOS IP SLAs technology is an embedded feature set in Cisco IOS software that allows you to analyze IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce occurrences of network congestion or outages. IP SLAs use active traffic monitoring—the generation of traffic in a continuous, reliable, and predictable manner—for measuring network performance. The accuracy of measured data is enhanced by enabling the IP SLAs responder, available in Cisco routers, on the destination device. This section also demonstrates how the data gathered using the UDP Jitter operation can be displayed and analyzed using the Cisco IOS CLI.

This section includes this information:

- [Information About the IP SLAs UDP Jitter Operation, page 9](#)
- [How to Configure the IP SLAs UDP Jitter Operation, page 10](#)
- [Configuration Example for the IP SLAs UDP Jitter Operation, page 25](#)

Information About the IP SLAs UDP Jitter Operation

To perform the tasks required to verify service levels using the IP SLAs UDP Jitter operation, you should understand the UDP jitter monitoring operation. The IP SLAs UDP Jitter monitoring operation was primarily designed to diagnose network suitability for real-time traffic applications such as voice over IP (VoIP), video over IP, or real-time conferencing.

Jitter means inter-packet delay variance. When multiple packets are sent consecutively from source to destination, for example, 10 ms apart, and if the network is behaving ideally, the destination should be receiving them 10 ms apart. But if there are delays in the network (like queueing, arriving through alternate routes, and so on) the arrival delay between packets might be greater than or less than 10 ms. Using this example, a positive jitter value indicates that the packets arrived greater than 10 ms apart. If

the packets arrive 12 ms apart, then positive jitter is 2 ms; if the packets arrive 8 ms apart, then negative jitter is 2 ms. For delay-sensitive networks like VoIP, positive jitter values are undesirable, and a jitter value of 0 is ideal.

However, the IP SLAs UDP Jitter operation does more than just monitor jitter. As the UDP Jitter operation includes the data returned by the IP SLAs UDP operation, the UDP Jitter operation can be used as a multipurpose data gathering operation. The packets IP SLAs generate carry packet sending sequence and receiving sequence information, and sending and receiving time stamps from the source and the operational target. Based on these, UDP Jitter operations are capable of measuring the following:

- Per-direction jitter (source to destination and destination to source)
- Per-direction packet-loss
- Per-direction delay (one-way delay)
- Round trip delay (average round trip time)

As the paths for the sending and receiving of data may be different (asymmetric), the per-direction data allow you to more readily identify where congestion or other problems are occurring in the network.

The UDP Jitter operation functions by generating synthetic (simulated) UDP traffic. The UDP Jitter operation sends N UDP packets, each of size S , sent T milliseconds apart, from a source router to a target router, at a given frequency of F . By default, ten packet-frames (N), each with a payload size of 10 bytes (S) are generated every 10 ms (T), and the operation is repeated every 60 seconds (F). Each of these parameters are user-configurable, so as to best simulate the IP service you are providing, or want to provide.

How to Configure the IP SLAs UDP Jitter Operation

This section contains the following procedures:

- [Configuring the IP SLAs Responder on the Destination Device, page 10](#) (required)
- [Configuring and Scheduling a UDP Jitter Operation on the Source Device, page 11](#)
- [Interpreting Results for UDP Jitter Operations, page 21](#)

Configuring the IP SLAs Responder on the Destination Device

Before configuring a UDP Jitter operation on the source device, the IP SLAs Responder must be enabled on the target device (the operational target). The IP SLAs Responder is available only on Cisco IOS software-based devices.

To enable the IP SLAs Responder, perform the following steps, beginning in privileged EXEC mode.

SUMMARY STEPS

1. **configure terminal**
2. **rtr responder**
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>configure terminal</code> Example: Router# <code>configure terminal</code>	Enters global configuration mode (from privileged EXEC mode)
Step 2	<code>rtr responder</code> Example: Router(config)# <code>rtr responder</code>	Enables the IP SLAs Responder.
Step 3	<code>end</code> Example: Router(config)# <code>end</code>	(Optional) Ends your configuration session and returns the CLI to privileged EXEC mode.

Configuring and Scheduling a UDP Jitter Operation on the Source Device

The IP SLAs operations function by generating synthetic (simulated) network traffic. A single IP SLAs operation (for example, IP SLAs operation 10) will repeat at a given frequency for the lifetime of the operation.

A single UDP Jitter operation consists of N UDP packets, each of size S , sent T milliseconds apart, from a source router to a target router, at a given frequency of F . By default, ten packets (N), each with an RTP payload size of 32 bytes (S), are generated every 20 ms (T), and the operation is repeated every 60 seconds (F). Each of these parameters are user-configurable, as shown here:

UDP Jitter Operation Parameter	Default	Configured Using:
Number of packets (N)	10 packets	type jitter command, num-packets option
Payload size per packet (S)	32 bytes	request-data-size command
Time between packets, in milliseconds (T)	20 ms	type jitter command, interval option
Elapsed time before the operation repeats, in seconds (F)	60 seconds	frequency command

Prerequisites

Use of the UDP Jitter operation requires that the IP SLAs Responder be enabled on the target Cisco device. To enable the Responder, perform the task in the [“Configuring the IP SLAs Responder on the Destination Device”](#) section on page 10

Time synchronization, such as that provided by NTP, is required between the source and the target device in order to provide accurate one-way delay (latency) measurements. To configure NTP on the source and target devices, perform the tasks in the [“Performing Basic System Management”](#) document (available on Cisco.com). Time synchronization is not required for the one-way jitter and packet loss measurements, however. If the time is not synchronized between the source and target devices, one-way jitter and packet loss data will be returned, but values of “0” will be returned for the one-way delay measurements provided by the UDP Jitter operation.

Before configuring any IP SLAs application, you can use the **show rtr application** command to verify that the operation type is supported on your software image.

Configuring and Scheduling a Basic UDP Jitter operation on the Source Device

Perform the following steps to configure and schedule a UDP Jitter operation, beginning in privileged EXEC mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **rtr operation-number**
4. **type jitter**
5. **frequency** (optional)
6. **exit**
7. **rtr schedule**
8. **end** (optional)
9. **show rtr configuration** (optional)
10. **copy running-config startup-config** (optional)

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable [<i>privilege-level</i>] Example: Router> enable Router#	Enters Privileged Exec mode from User Exec mode.
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	rtr operation-number Example: Router(config)# rtr 10	Specifies a unique identification number for the operation to be configured, and enters RTR configuration mode.

Command or Action	Purpose
<p>Step 3</p> <pre>type jitter dest-ipaddr {hostname ip-address} dest-port port-number [num-packets number-of-packets] [interval inter-packet-interval]</pre> <p>Example: Router(config-rtr)# type jitter dest-ipaddr 172.29.139.134 dest-port 5000</p>	<p>Configures the operation as a Jitter operation, and configures characteristics for the operation.</p> <ul style="list-style-type: none"> • Use the dest-ipaddr keyword to specify the IP address or IP host name of the destination for the UDP Jitter operation. • Use the dest-port keyword and associated option to specify the destination port number, in the range from 1 to 65535. • The default number of packets (num-packets) sent is 10. The default interval between packets is 20 milliseconds. • After entering this command, the command-line interface (CLI) enters RTR Jitter configuration mode to allow you to specify optional characteristics for the operation. <p>Note Only partial syntax used in this example. For more details, see the <i>Cisco IOS Configuration Fundamentals and Network Management Command Reference</i>, 12.3T.</p>
<p>Step 4</p> <pre>frequency seconds</pre> <p>Example: Router(config-rtr-jitter)# frequency 30</p>	<p>(Optional) Specifies the amount of time between probe operations. By default, UDP Jitter operations are sent every 60 seconds for the lifetime of the operation.</p> <ul style="list-style-type: none"> • Use the <i>seconds</i> argument to specify the number of seconds before the start of the next operational cycle. Range: 1 to 12604800. Default: 60.
<p>Step 5</p> <pre>exit</pre> <p>Example: Router(config-rtr-jitter)# exit Router(config)#</p>	<p>Exits from RTR configuration mode and operational submenu, and returns the CLI to global configuration mode.</p>

Command or Action	Purpose
<p>Step 6</p> <pre>rtr schedule operation-number [life {forever seconds}] [start-time {hh:mm[:ss] [month day day month] pending now after hh:mm:ss] [ageout seconds]</pre> <p>or</p> <pre>rtr schedule operation-number [life seconds] start-time {hh:mm[:ss] [month day day month] [ageout seconds] recurring</pre> <p>Example: Router(config)# rtr schedule 10 life 300 start-time after 00:05:00</p> <p>or</p> <pre>Router(config)# rtr schedule 15 start-time 01:30:00 recurring</pre>	<p>Schedules the start time of the operation. You can configure a basic schedule, configure a recurring schedule, or schedule multiple operations using group scheduling.</p> <ul style="list-style-type: none"> • Use the optional life forever syntax to configure the operation to run indefinitely. Use the optional life seconds syntax to configure the lifetime of the operation, in seconds. The default lifetime of an operation is 3600 seconds (one hour). • Use the optional start-time time, month, and day syntax to specify a time for the operation to start. • Use the optional start-time pending syntax to configure the operation to remain in a pending (un-started) state. This is the default value. 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. • Use the optional start-time now syntax to indicate that the operation should start immediately. • Use the optional start-time after syntax to specify the amount of time, in hours and seconds, that should pass before starting the operation. • Use the optional ageout keyword and <i>seconds</i> argument to specify the number of seconds to keep the operation in memory when it is not actively collecting information. The default value of 0 seconds means that the operation never times out. <p>Use the rtr schedule command with the recurring option to configure the operation to restart at a certain time every day. If the recurring option is used, the start-time syntax is required, and the lifetime value should not be more than 24 hours (life 86398 or less). The recurring option is only available in Cisco IOS Releases 12.3(8)T or 12.2(25)S or later.</p>
<p>Step 7</p> <pre>end</pre> <p>Example: Router(config)# end Router# </p>	<p>(Optional) Ends the current configuration session and returns the CLI to privileged EXEC mode.</p>

	Command or Action	Purpose
Step 8	<pre>show rtr configuration [operation-number] or show running-config</pre> <p>Example: Router# show rtr configuration 10 OR Router# show running-config begin rtr </p>	<p>(Optional) Displays the current IP SLAs (RTR) configuration so you can verify the configuration you just performed.</p> <ul style="list-style-type: none"> The <i>operation-number</i> argument can be used to show you only the configuration of the specified operation.
Step 9	<pre>copy running-config startup-config</pre> <p>Example: Router# copy run start </p>	<p>(Optional) Saves the running configuration to the startup configuration file.</p>

Examples

The following example shows the configuration of the IP SLAs UDP Jitter operation number 10 that will start in 5 minutes and run for 5 minutes.

```
rtr 1
  type jitter dest-ipaddr 172.29.139.134 dest-port 5000 num-packets 20
  frequency 30
rtr schedule 1 life 300 start-time after 00:05:00
```

Configuring and Scheduling a UDP Jitter Operation with Additional Characteristics

Perform the following steps to configure and schedule a UDP Jitter operation, beginning in privileged EXEC mode.

Restrictions

The IP SLAs UDP Jitter operation does not support the IP SLAs History feature (statistics history buckets) because of the large data volume involved with UDP Jitter operations. This means that the following commands are not supported for UDP Jitter operations: **buckets-of-history-kept**, **filter-for-history**, **lives-of-history-kept**, **samples-of-history-kept**, and **show rtr history**.

The MIB used by IP SLAs (CISCO-RTTMON-MIB) limits the hours-of-statistics kept for the UDP Jitter operation to two hours. Configuring a larger value using the **hours-of-statistics** *hours* global configuration change will not increase the value beyond two hours.

However, the Data Collection MIB can be used to collect historical data for the operation. See the CISCO-DATA-COLLECTION-MIB (available from <http://www.cisco.com/go/mibs>) and the “Periodic MIB Data Collection and Transfer Mechanism” document for more information.

SUMMARY STEPS

1. **configure terminal**
2. **rtr operation-number**
3. **type jitter**
4. **dest-ipaddr** (optional)
5. **dest-port** (optional)
6. **frequency** (optional)
7. **enhanced-history** (optional)
8. **owner** (optional)
9. **request-data-size** (optional)
10. **tag** (optional)
11. **hours-of-statistics kept** (optional)
12. **threshold** (optional; not recommended)
13. **timeout** (optional)
14. **tos** (optional)
15. **verify-data** (optional)
16. **vrf** (optional)
17. **exit**
18. **rtr schedule**
19. **end** (optional)
20. **show rtr configuration** (optional)
21. **copy running-config startup-config** (optional)

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	rtr operation-number Example: Router(config)# rtr 10	Specifies a unique identification number for the operation to be configured, and enters RTR configuration mode.

Command or Action	Purpose
<p>Step 3</p> <pre>type jitter dest-ipaddr {hostname ip-address} dest-port port-number [source-ipaddr {name ip-address}] [source-port port-number] [num-packets number-of-packets] [interval inter-packet-interval] [control {enable disable}]</pre> <p>Example: Router(config-rtr)# type jitter dest-ipaddr 172.29.139.134 dest-port 5000</p>	<p>Configures the operation as a Jitter operation, and configures characteristics for the operation.</p> <ul style="list-style-type: none"> • Use the dest-ipaddr keyword to specify the IP address or IP host name of the destination for the UDP Jitter operation. • Use the dest-port keyword and associated option to specify the destination port number, in the range from 1 to 65535. • All other keywords and arguments are optional. See the command reference document for more information. The default number of packets (num-packets) sent is 10. The default interval between packets is 20 milliseconds. • The control disable keyword combination should only be used if you are disabling the IP SLAs control protocol on both the source and target routers. The IP SLAs control protocol is enabled by default. • After entering this command, the command-line interface (CLI) enters RTR Jitter configuration mode to allow you to specify optional characteristics for the operation.
<p>Step 4</p> <pre>dest-ipaddr ip-address</pre>	<p>(Optional) Specifies the destination IP address for the operation.</p> <ul style="list-style-type: none"> • Use of this command will overwrite the IP address specified in the syntax of the type jitter command. • This command allows you to change the target device for the operation without disabling and reenabling the operation type.
<p>Step 5</p> <pre>dest-port port-number</pre>	<p>(Optional) The destination port number for the operation.</p> <ul style="list-style-type: none"> • Use of this command will overwrite the port number specified in the syntax of the type jitter command. • This command allows you to change the target port for the operation without disabling and reenabling the operation type.
<p>Step 6</p> <pre>frequency seconds</pre> <p>Example: Router(config-rtr-jitter)# frequency 30</p>	<p>(Optional) Specifies the amount of time between probe operations. By default, jitter probe operations are sent every 60 seconds for the lifetime of the operation.</p> <ul style="list-style-type: none"> • Use the <i>seconds</i> argument to specify the number of seconds before the start of the next operational cycle. Range: 1 to 12604800. Default: 60.
<p>Step 7</p> <pre>enhanced-history interval seconds buckets number-of-buckets</pre> <p>Example: Router(config-rtr-jitter)# enhanced-history interval 900 buckets 100</p>	<p>(Optional) Enables enhanced history collection for the Jitter operation.</p> <ul style="list-style-type: none"> • To view collected enhanced history statistics, use the show rtr enhanced-history command. <p>Note Standard IP SLAs history statistics are not available for the Jitter operation.</p>
<p>Step 8</p> <pre>owner owner-id</pre> <p>Example: Router(config-rtr-jitter)# owner admin</p>	<p>(Optional) Allows you to specify a process owner for the operation, as a free text designation.</p> <ul style="list-style-type: none"> • This option may be helpful in identifying who originated an operation in an environment where many operations are being run.

	Command or Action	Purpose
Step 9	<p>request-data-size <i>bites</i></p> <p>Example: Router(config-rtr-jitter)# request-data-size 64</p>	<p>(Optional) Sets the data size in the payload of the operation's request packets.</p> <ul style="list-style-type: none"> This command applies only to the DLSw and Jitter operations. The default for DLSw operations is 0 bytes. The range is 0 to 16384 bytes. The default request-size for Jitter operations is 32 bytes. The range is 16 to 1500 bytes.
Step 10	<p>tag <i>text</i></p> <p>Example: Router(config-rtr-jitter)# tag TelnetPollServer1</p>	<p>(Optional) Allows you to specify a label to the operation, as a free text designation.</p> <ul style="list-style-type: none"> This option may be helpful in grouping multiple operations from the same or different routers.
Step 11	<p>hours-of-statistics-kept <i>hours</i></p> <p>Example: Router(config-rtr-jitter)# hours-of-statistics-kept 4</p>	<p>(Optional) The number of hours for which statistics are kept.</p> <ul style="list-style-type: none"> By default, the router will retain statistics for the last two hours the operation was running. If the operation runs more than the specified number of hours, the oldest data will be replaced by newer data. If the operation stops running, the data will be kept indefinitely, but for only the last <i>x</i> hours the operation was running. (For example, 2 hours worth of data will be kept in memory indefinitely.)
Step 12	<p>threshold <i>milliseconds</i></p> <p>Example: Router(config-rtr-jitter)# timeout 10000</p>	<p>(Not recommended) Configures the upper-limit threshold value (or rising threshold) that will trigger an IP SLAs reaction event.</p> <ul style="list-style-type: none"> The functionality of this command has been replaced by the threshold-value <i>upper-limit lower-limit</i> syntax in the rtr reaction-configuration command in Cisco IOS Release 12.3(7)T. Use of the threshold command is not recommended, as support for this command will be removed in an upcoming release.
Step 13	<p>timeout <i>milliseconds</i></p> <p>Example: Router(config-rtr-jitter)# timeout 10000</p>	<p>(Optional) Sets the amount of time that the specified IP SLAs operation waits for a response from its request packet.</p> <p>Use the <i>milliseconds</i> argument to specify the number of milliseconds that the operation waits to receive a response.</p>
Step 14	<p>tos <i>number</i></p> <p>Example: Router(config-rtr-jitter)# tos 160</p>	<p>(Optional) Sets the Type Of Service byte value (including IP Precedence data) for request packets.</p> <ul style="list-style-type: none"> The ToS byte can be converted to a Differentiated Serve Code Point (DSCP) value, but you cannot enter the DSCP value directly. To use a DSCP value, multiply it by 4 and enter the result as the <i>number</i> argument. For example, the DSCP value 46 is ToS value 184.
Step 15	<p>verify-data</p> <p>Example: Router(config-rtr-jitter)# verify-data</p>	<p>(Optional) Configures IP SLAs to check each probe response for data corruption.</p> <p>Note Only use the verify-data command when you suspect corruption may be an issue.</p>

Command or Action	Purpose
<p>Step 16 <code>vrf vrf-name</code></p> <p>Example: Router(config-rtr-jitter)# vrf vpn-A</p>	<p>(Optional) Configures the Jitter operation to run over a specific VPN by binding the operation to a specific VRF table.</p>
<p>Step 17 <code>exit</code></p> <p>Example: Router(config-rtr-jitter)# exit Router(config)#</p>	<p>Exits from RTR configuration mode and operational submode, and returns the CLI to global configuration mode.</p>
<p>Step 18 <code>rtr schedule operation-number</code> [life {forever <i>seconds</i>}] [start-time {<i>hh:mm[:ss]</i> [<i>month day</i> <i>day month</i>] pending now after <i>hh:mm:ss</i>] [ageout <i>seconds</i>] [recurring]</p> <p>or</p> <p><code>rtr schedule operation-number</code> [life <i>seconds</i>] start-time {<i>hh:mm[:ss]</i> [<i>month day</i> <i>day month</i>]} [ageout <i>seconds</i>] recurring</p> <p>Example: Router(config)# rtr schedule 5 start-time now life forever</p> <p>or</p> <p>Router(config)# rtr schedule 15 start-time 01:30:00 recurring</p>	<p>Schedules the start time of the operation. You can configure a basic schedule, configure a recurring schedule, or schedule multiple operations using group scheduling.</p> <ul style="list-style-type: none"> • Use the optional life forever syntax to configure the operation to run indefinitely. Use the optional life seconds syntax to configure the lifetime of the operation, in seconds. The default lifetime of an operation is 3600 seconds (one hour). • Use the optional start-time time, month, and day syntax to specify a time for the operation to start. • Use the optional start-time pending syntax to configure the operation to remain in a pending (un-started) state. This is the default value. 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. • Use the optional start-time now syntax to indicate that the operation should start immediately. • Use the optional start-time after syntax to specify the amount of time, in hours and seconds, that should pass before starting the operation. • Use the optional ageout keyword and <i>seconds</i> argument to specify the number of seconds to keep the operation in memory when it is not actively collecting information. The default value of 0 seconds means that the operation never times out. • Use the rtr schedule command with the recurring option to configure the operation to restart at a certain time every day. If the recurring option is used, the start-time syntax is required, and the lifetime value should not be more than 24 hours (life 86398 or less). The recurring option is only available in Cisco IOS Releases 12.3(8)T or 12.2(25)S or later.
<p>Step 19 <code>end</code></p> <p>Example: Router(config)# end Router#</p>	<p>(Optional) Ends the current configuration session and returns the CLI to privileged EXEC mode.</p>

Command or Action	Purpose
<p>Step 20 <code>show rtr configuration</code> <code>[operation-number]</code></p> <p>or</p> <p><code>show running-config</code></p> <p>Example: Router# show rtr configuration 10 OR Router# show running-config begin rtr</p>	<p>(Optional) Displays the current IP SLAs (RTR) configuration so you can verify the configuration you just performed.</p> <ul style="list-style-type: none"> The <i>operation-number</i> argument can be used to show you only the configuration of the specified operation.
<p>Step 21 <code>copy running-config startup-config</code></p> <p>Example: Router# copy run start</p>	<p>(Optional) Saves the running configuration to the startup configuration file.</p>

Examples

In the following example, two operations are configured as UDP Jitter operations, with operation 2 starting five seconds operation 1. Both operations will run indefinitely.

```
!
rtr 1
  type jitter dest-ipaddr 20.0.10.3 dest-port 65051 num-packets 20
  request-data-size 160
  tos 128
  frequency 30
rtr schedule 1 start-time after 00:05:00
rtr 2
  type jitter dest-ipaddr 20.0.10.3 dest-port 65052 num-packets 20 interval 10
  request-data-size 20
  tos 64
  frequency 30
rtr schedule 2 start-time after 00:05:05
!
```

What to Do Next

Allow the statistics to be gathered for the desired amount of time and then proceed to the [“Interpreting Results for UDP Jitter Operations”](#) section to display and interpret the results.

Interpreting Results for UDP Jitter Operations

The function of the IP SLAs monitoring operations is to return statistics (aggregated data) on the performance of the network. To view and interpret the results of the UDP Jitter operation use the **show** commands listed in the following steps.

To help you interpret the output, a table explaining the significant fields is located after the output for each command. Checking the output for fields that correspond to criteria in your service level agreement will help you determine whether the service level metrics are acceptable.

The UDP Jitter operation provides the following statistics:

- jitter statistics — useful for telephony and multi-media conferencing
- packet loss and packet sequencing statistics — useful for telephony, multimedia conferencing, streaming media, and other low latency data requirements
- one-way latency/ delay statistics — useful for telephony, multi-media conferencing, and streaming media

Prerequisites

Complete the “[Configuring the IP SLAs Responder on the Destination Device](#)” section on page 10, the “[Configuring and Scheduling a UDP Jitter Operation on the Source Device](#)” section on page 11, and allow statistics to be gathered for the desired period of time before performing this task.

SUMMARY STEPS

1. **show rtr operational-state** [*operation-id*]
2. **show rtr totals-statistics** [*operation-id*]
3. **show rtr collection-statistics** [*operation-id*]

DETAILED STEPS

Step 1 show rtr operational-state

Use this command to display the state of the UDP Jitter IP SLAs operation and the statistics that were gathered for the last iteration of the operation.

```
Router# show rtr operational-state 1

      Current Operational State

Entry Number:1
Modification Time: 11:20:24.627 UTC on Jun 17 2004
Number of operations attempted: 2
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 1
Latest operation start time: *11:20:54.624 UTC Mon Jun 17 2004
Latest operation return code: OK

RTT Values:
NumOfRTT:10      RTTSum:32      RTTSum2:128
```

```

Packet Loss Values:
PacketLossSD:0 PacketLossDS:0
PacketOutOfSequence:0 PacketMIA:0 PacketLateArrival:0
InternalError:0 Busies:0

Jitter Values:
MinOfPositivesSD:4 MaxOfPositivesSD:4
NumOfPositivesSD:2 SumOfPositivesSD:8 Sum2PositivesSD:32
MinOfNegativesSD:4 MaxOfNegativesSD:4
NumOfNegativesSD:1 SumOfNegativesSD:4 Sum2NegativesSD:16
MinOfPositivesDS:0 MaxOfPositivesDS:0
NumOfPositivesDS:0 SumOfPositivesDS:0 Sum2PositivesDS:0
MinOfNegativesDS:4 MaxOfNegativesDS:4
NumOfNegativesDS:1 SumOfNegativesDS:4 Sum2NegativesDS:16
    
```

Table 1 describes the fields shown in the display.

Table 1 show rtr operational-state Field Descriptions for UDP Jitter

Field	Description
Entry number	IP SLAs operation number.
Modification time:	Time and date the operation was created. An asterisk before the time (e.g. *03:34:44.000) means that time is not synchronized.
Number of operations attempted:	Number of active measurements sent across the network.
Number of operations skipped:	Number of operations that could not be activated across the network.
Current seconds left in Life:	Time, in seconds, before the operation stops activating. The life of the operation is a configurable parameter.
Operational state of entry:	Indicates whether the operation is active and measuring the network.
Last time this entry was reset:	Indicates whether the operation has been reset by displaying the text, Never, or the time when the last reset occurred. When an operation is reset, all the saved statistics are deleted.
Connection loss occurred	Indicates whether any connection loss has occurred from a timeout or other network issue. If no connection has been lost, FALSE is displayed.
Timeout occurred	Indicates whether a timeout occurred after the source attempted to connect to the destination. If no timeout has occurred, FALSE is displayed.
Over thresholds occurred	Indicates whether a threshold was set and exceeded. If no threshold has been set or exceeded, FALSE is displayed.
Latest RTT (milliseconds)	Round-trip time (RTT), in milliseconds, of the last iteration of the operation.
Latest operation start time	Time of the last measurement.
Latest operation return code	Indicates the operation status.
Jitter values:	The statistics that were gathered for the last iteration of the operation. For an explanation of these fields, see Table 2 on page 23.

Step 2 show rtr totals-statistics

Use this command to display the age of statistics, and number of initiations for the operation.

```

Router# show rtr totals-statistics 10

Statistic Totals
    
```

```

Entry Number: 10
Start Time Index: 22:19:21.000 UTC Thur Sept 16 2004
Age of Statistics Entry (hundredths of seconds): 360000
Number of Initiations: 60

```

Step 3 show rtr collection-statistics

This command shows information collected over the past two hours, unless a different amount of time was specified using the **hours-of-statistics-kept** command (no more than two hours can be stored for UDP Jitter operations). Although the output for the **show rtr operational-state** is similar to the output for this command, the output for the **show rtr operational-state** is only for the last completed operation, not aggregated statistics of all operations for the last two hours.

The following is sample output from the **show rtr collection-statistics** command, where operation 1 is a Jitter operation which includes One Way reporting Values:

```

Router# 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

```

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. OW stands for One Way. [Table 2](#) describes the significant fields shown in this output.

Table 2 show rtr collection-statistics Field Descriptions for UDP Jitter

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.

Table 2 *show rtr collection-statistics Field Descriptions for UDP Jitter (continued)*

Field	Description
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.
One Way Values	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.
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 the OWMinSD and OWMaxSD values.
OWSum2SD	Sum of the squares of the OWMinSD and OWMaxSD values.

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

Examples

The following sample output shows the configuration of all the IP SLAs parameters (including defaults) for the operation 5.

```
Router# show rtr configuration 5

Complete configuration Table (includes defaults)
Entry number: 5
Owner: jdoe
Tag: FLL-RO
Type of operation to perform: Jitter
Target address: 172.29.139.134
Source address: 0.0.0.0
Target port: 5000
Source port: 0
Request size (ARR data portion): 160
Operation timeout (milliseconds): 1000
Type Of Service parameters: 128
```

```

Verify data: No
Data pattern:
Vrf Name:
Control Packets: enabled
Operation frequency (seconds): 30
Next Scheduled Start Time: Start Time already passed
Group Scheduled: FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Number of statistic hours kept: 2
Number of statistic distribution buckets kept: 1
Statistic distribution interval (milliseconds): 20
Enhanced History:
Aggregation Interval:60 Buckets:2
Number of history Lives kept: 0
Number of history Buckets kept: 15
History Filter Type: None

```

Troubleshooting Tips

- If the UDP Jitter operation is not running and generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in RTR mode) to enable data verification. When enabled, each operation response is checked for corruption. Use the **verify-data** command with caution during normal operations because it generates unnecessary overhead.
- Use the **debug rtr trace** and **debug rtr error** commands to help troubleshoot issues with the UDP Jitter operation.

Configuration Example for the IP SLAs UDP Jitter Operation

In the following example, two operations are configured as UDP Jitter operations, with operation 2 starting five seconds after the first operation. Both operations will run indefinitely.

```

!
rtr responder
rtr 1
  type jitter dest-ipaddr 20.0.10.3 dest-port 65051 num-packets 20
  request-data-size 160
  tos 128
  frequency 30
rtr schedule 1 start-time after 00:05:00
rtr 2
  type jitter dest-ipaddr 20.0.10.3 dest-port 65052 num-packets 20 interval 10
  request-data-size 20
  tos 64
  frequency 30
rtr schedule 2 start-time after 00:05:05
!

```

Command Reference

These commands are included on the following pages:

- [frequency \(RTR\), page 27](#)
- [rtr, page 29](#)
- [rtr responder, page 31](#)
- [type jitter, page 32](#)

frequency (RTR)

To set the rate at which a specified IP SLAs operation repeats, use the **frequency** command in RTR configuration mode. To return to the default value, use the **no** form of this command.

frequency *seconds*

no frequency

Syntax Description	<i>seconds</i>	Number of seconds between the IP SLAs probes.
--------------------	----------------	---

Defaults	60 seconds
----------	------------

Command Modes	RTR Jitter Configuration Mode (config-rtr-jitter) RTR IP/ICMP Echo Configuration Mode (config-rtr-echo) RTR UDP Echo Configuration Mode (config-rtr-udp) RTR HTTP Configuration Mode (config-rtr-http)
---------------	---

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines The IP SLAs operations function by generating synthetic (simulated) network traffic. A single IP SLAs operation (for example, IP SLAs operation 10) will repeat at a given frequency for the lifetime of the operation.

For example, a UDP Jitter operation with a frequency of 60 repeats by sending a collection of packets simulating network traffic every 60 seconds for the lifetime of the operation. The default synthetic traffic in a UDP Jitter operation consists of 10 packets sent 20 milliseconds apart. The operation is then repeated, by default, 60 seconds later.

If an individual IP SLAs operation takes longer to execute than the specified frequency value, a statistics counter called “busy” is incremented rather than immediately repeating the operation.



Note

We recommend that you do not set the frequency value to less than 60 seconds for the following reasons: It is not needed when keeping statistics, and it can slow down the network because of the potential overhead that numerous operations can cause.

The value specified for the **frequency** command cannot be less than the value specified for the **timeout** RTR configuration mode command.

Examples

The following example configures the IP SLAs IP/ICMP Echo operation (operation 10) to repeat every 90 seconds:

```
Router(config)# rtr 10
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.1.176
Router(config-rtr-echo)# frequency 90
```

Related Commands

Command	Description
rtr	Specifies an IP SLAs operation I.D. and enters RTR configuration mode.
timeout	Sets the amount of time the IP SLAs operation waits for a response from its request packet.

rtr

To begin configuring an IP SLAs operation by entering RTR configuration mode, use the **rtr** command in global configuration mode. To remove all configuration information for an operation, including the schedule of the operation, reaction configuration, and reaction triggers, use the **no** form of this command.

rtr *operation-number*

no rtr *operation-number*

Syntax Description	<i>operation-number</i>	Operation number used for the identification of the IP SLAs operation you wish to configure.
---------------------------	-------------------------	--

Defaults	Disabled.
-----------------	-----------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.2	This command was introduced.
	12.2(11)T, 12.2(25)S	The maximum number of operations was increased from 500 to 2000 (SAA Engine II introduced).
	12.3(11)T	IP SLAs replaces SAA.

Usage Guidelines The **rtr** command is used to configure IP SLAs operations. Use this command to specify an identification number for the operation you are about to configure. After you enter this command, you will enter the RTR configuration mode, indicated by the (config-rtr) router prompt. The “Related Commands” table lists the commands you can use in RTR configuration mode.

IP SLAs allow a maximum of 2000 operations.

Debugging is supported only on the first 32 operation numbers.

After you configure a operation, you must schedule the operation. For information on scheduling a operation, refer to the **rtr schedule** global configuration command. You can also optionally set reaction triggers for the operation. For information on reaction triggers, refer to the **rtr reaction-configuration** and **rtr reaction-trigger** global configuration commands.



Note

After you schedule an operation with the **rtr schedule** global configuration command, you cannot modify the configuration of the operation. To modify the configuration of the operation after it is scheduled, use the **no rtr** command. You can now reenter the operation’s configuration with the **rtr** command.

To display the current configuration settings of the operation, use the **show rtr configuration EXEC** command.

Examples

In the following example, IP SLAs operation 5 is configured as a UDP Echo operation. The operation is then configured to start immediately and run forever.

```
Router(config)# rtr 5
Router(config-rtr)# type udpEcho dest-ipaddr 172.29.139.134 dest-port 5000
Router(config-rtr-udpEcho)# frequency 30
Router(config-rtr-udpEcho)# exit
Router(config)# rtr schedule 5 start-time now life forever.
```

Related Commands

Command	Description
buckets-of-history-kept	Sets the number of history buckets that are kept during an IP SLAs operation's lifetime.
distributions-of-statistics-kept	Sets the number of statistic distributions kept per hop during an IP SLAs operation's lifetime.
filter-for-history	Defines the types of information to be kept in the history table for IP SLAs operations.
frequency	Sets the frequency at which the operation should execute.
hops-of-statistics-kept	Sets the number of hops for which statistics are maintained per path for the IP SLAs operation.
hours-of-statistics-kept	Sets the number of hours for which statistics are maintained for IP SLAs operations.
lives-of-history-kept	Sets the number of lives maintained in the history table for an IP SLAs operation.
lsr path	Specifies the path on which to measure the ICMP Echo response time.
owner	Configures the SNMP owner of an IP SLAs operation.
paths-of-statistics-kept	Sets the number of paths for which statistics are maintained per hour for an IP SLAs operation.
request-data-size	Sets the protocol data size in the payload of an operation's request packet.
response-data-size	Sets the protocol data size in the payload of an operation's response packet.
samples-of-history-kept	Sets the number of entries kept in the history table for an IP SLAs operation.
statistics-distribution-interval	Sets the time interval for each statistical distribution.
tag	Logically links IP SLAs operations together in a group.
threshold	Sets the rising threshold (hysteresis) that generates a reaction event and stores history information for the probe.
timeout	Sets the amount of time an IP SLAs operation waits for a response from its request packet.
tos	Defines the IP type of service for request packets of IP SLAs operations.
type dlsW	Configures an IP SLAs DLSw operation.
type tcpConnect	Defines an IP SLAs TCP Connect operation.
verify-data	Checks each IP SLAs operation response for corruption.

rtr responder

To enable the IP SLAs Responder on a destination (operational target) device, use the **rtr responder** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

rtr responder

no rtr responder

Syntax Description This command has no arguments or keywords.

Defaults Disabled.

Command Modes Global configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced.

Usage Guidelines This command is used on the destination device for IP SLAs operations to enable the sending of receiving of RTR Control packets. Enabling the IP SLAs Responder allows the generation of packet loss statistics on the device sending IP SLAs operations.

Examples The following example enables the IP SLAs Responder:

```
Router(config)# rtr responder
```

Related Commands	Command	Description
	rtr responder type tcpConnect	Enables the IP SLAs Responder for TCP Connect operations.
	rtr responder type udpEcho	Enables the IP SLAs Responder for UDP Echo and Jitter operations.

type jitter

To configure an IP SLAs UDP Jitter operation, use the **type jitter** command in RTR configuration mode. To disable an existing UDP Jitter operation, use the **no** form of this command.

```
type jitter dest-ipaddr {hostname | ip-address} dest-port port-number [source-ipaddr {name | ip-address}] [source-port port-number] [control {enable | disable}] [num-packets number-of-packets] [interval inter-packet-interval]
```

```
no type jitter dest-ipaddr {name | ip-address} dest-port port-number [source-ipaddr {name | ip-address}] [source-port port-number] [control {enable | disable}] [num-packets number-of-packets] [interval inter-packet-interval]
```

Syntax Description

dest-ipaddr {hostname ip-address}	Specifies the target destination for the operation, as an IP address or an IP host name.
dest-port port-number	Specifies the destination port number. Range: 1 - 65535.
source-ipaddr {name ip-address}	(Optional) Explicitly specifies the source address that will be used in the operation, as an IP address, or as an IP host name.
source-port port-number	(Optional) Specifies the port that the operation should be sent from (source port), using the port number.
control {enable disable}	(Optional) Enables or disables the IP SLAs control protocol. The IP SLAs control protocol sends a control message to the destination port prior to sending any operational probe packets. <ul style="list-style-type: none"> The control disable option should only be used if you are disabling the IP SLAs control protocol on both the source and target routers. The IP SLAs control protocol is enabled by default.
num-packets number-of-packets	(Optional) Number of packets, as specified in the <i>number-of-packets</i> argument. The default number of packets sent is 10.
interval inter-packet-interval	(Optional) Interpacket interval, in milliseconds. The default interval between packets is 20 milliseconds.

Defaults

No IP SLAs operation type is configured for the operation number (**rtr** I.D.) being configured.

Command Modes

RTR configuration mode (config-rtr)

Command History

Release	Modification
12.0(5)T, 12.0(8)S, 12.2(14)S, 12.1E	This command was introduced.
12.2(2)T, 12.2(14)S	Support for one-way delay measurements (one-way latency) was added for the Jitter operation.

Usage Guidelines

The **type jitter** command configures an IP SLAs UDP Jitter monitoring operation. In addition to measuring UDP round trip time, the Jitter operation measures per-direction packet-loss and jitter (inter-packet delay variance). Packet loss is a critical element in service level agreements, and jitter statistics are useful for analyzing traffic in VoIP networks.

You must enable the IP SLAs Responder on the target router (using the **rtr responder** command on the target device) before you can configure a Jitter operation. Prior to sending a operation packet to the responder, the IP SLAs subsystem sends a control message to the IP SLAs Responder to enable the destination port.

You must configure the type of operation before you can configure any of the other characteristics of the operation. After entering this command, the command-line interface (CLI) enters RTR Jitter configuration mode to allow you to specify optional characteristics for the operation. Other characteristics of the Jitter operation, such as request-data-size, are configured in RTR Jitter configuration mode.



Note

Standard IP SLAs history statistics are not available for UDP Jitter operations. History for Jitter operations can be collected using the enhanced history option.

Examples

In the following example, operation 6 is created and configured as a UDP Jitter operation using the destination IP address 172.30.125.15, the destination port number 2000, 20 packets, and an interval of 20:

```
Router(config)# rtr 6
Router(config-rtr)# type jitter dest-ip 172.30.125.15 dest-port 2000 num-packets 20
interval 20
Router(config-rtr-jitter)#
```

Related Commands

Command	Description
request-data-size	Sets the payload size for IP SLAs operation requests.
rtr	Specifies an IP SLAs operation I.D. and enters RTR configuration mode.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
or view the digital edition at this URL:
<http://ciscoiq.texterity.com/ciscoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

© 2006 Cisco Systems, Inc. All rights reserved.

