



EFT REVIEW DRAFT – CISCO CONFIDENTIAL

Configuring Cisco IOS IP SLAs TCP Connect Operations

First Published: August 14, 2006

Last Updated: February 14, 2011

This module describes how to configure a Cisco IOS IP Service Level Agreements (SLAs) TCP Connect operation to measure the response time taken to perform a TCP Connect operation between a Cisco router and devices using IPv4 or IPv6. TCP Connect accuracy is enhanced by using the IP SLAs Responder at the destination Cisco router. This module also demonstrates how the results of the TCP Connect operation can be displayed and analyzed to determine how the connection times to servers and hosts within your network can affect IP service levels. The TCP Connect operation is useful for measuring response times for a server used for a particular application or connectivity testing for server availability.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for the IP SLAs TCP Connect Operation](#)” section on page 13.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Information About the IP SLAs TCP Connect Operation](#), page 2
- [How to Configure the IP SLAs TCP Connect Operation](#), page 3
- [Configuration Examples for the IP SLAs TCP Connect Operation](#), page 10
- [Additional References](#), page 11



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2006-2010 Cisco Systems, Inc. All rights reserved.

EFT REVIEW DRAFT – CISCO CONFIDENTIAL

- [Feature Information for the IP SLAs TCP Connect Operation, page 13](#)

Information About the IP SLAs TCP Connect Operation

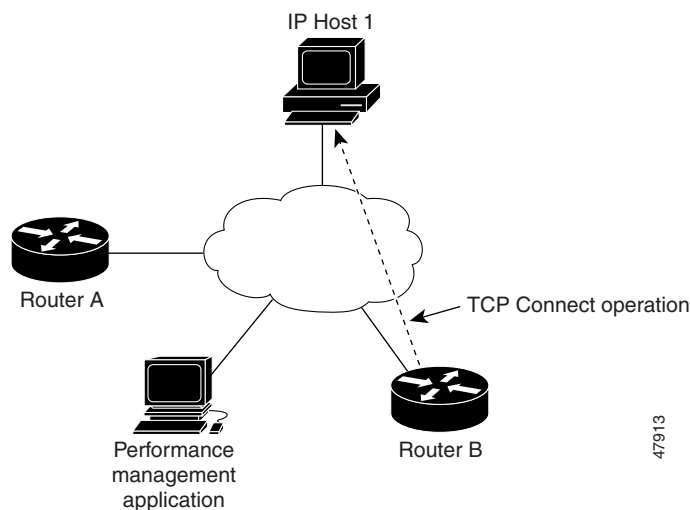
- [TCP Connect Operation, page 2](#)

TCP Connect Operation

The IP SLAs TCP Connect operation measures the response time taken to perform a TCP Connect operation between a Cisco router and devices using IP. TCP is a transport layer (Layer 4) Internet protocol that provides reliable full-duplex data transmission. The destination device can be any device using IP or an IP SLAs Responder.

In [Figure 1](#) Router B is configured as the source IP SLAs device and a TCP Connect operation is configured with the destination device as IP Host 1.

Figure 1 TCP Connect Operation



Connection response time is computed by measuring the time taken between sending a TCP request message from Router B to IP Host 1 and receiving a reply from IP Host 1.

TCP Connect accuracy is enhanced by using the IP SLAs Responder at the destination Cisco device. If the destination router is a Cisco router, then IP SLAs makes a TCP connection to any port number that you specified. If the destination is not a Cisco IP host, then you must specify a known destination port number such as 21 for FTP, 23 for Telnet, or 80 for an HTTP server.

Using the IP SLAs Responder is optional for a TCP Connect operation when using Cisco devices. The IP SLAs Responder cannot be configured on non-Cisco devices.

TCP Connect is used to test virtual circuit availability or application availability. Server and application connection performance can be tested by simulating Telnet, SQL, and other types of connection to help you verify your IP service levels.

EFT REVIEW DRAFT – CISCO CONFIDENTIAL

How to Configure the IP SLAs TCP Connect Operation

- [Configuring the IP SLAs Responder on the Destination Device, page 3](#) (optional)
- [Configuring and Scheduling a TCP Connect Operation on the Source Device, page 4](#) (required)

Configuring the IP SLAs Responder on the Destination Device

Prerequisites

If you are using the IP SLAs Responder, ensure that the networking device to be used as the Responder is a Cisco device and that you have connectivity to that device through the network.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip sla responder`
or
`ip sla responder tcp-connect ipaddress ip-address port port-number`
4. `exit`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# <code>configure terminal</code>	Enters global configuration mode.

EFT REVIEW DRAFT – CISCO CONFIDENTIAL

	Command or Action	Purpose
Step 3	<pre>ip sla responder or ip sla responder tcp-connect ipaddress ip-address port port</pre> <p>Example: Router(config)# ip sla responder or</p> <p>Example: Router(config)# ip sla responder tcp-connect ipaddress 172.29.139.132 port 5000 </p>	<p>(Optional) Temporarily enables IP SLAs Responder functionality on a Cisco device in response to control messages from source.</p> <p>or</p> <p>(Optional) Required only if protocol control is disabled on source. Permanently enables IP SLAs Responder functionality on specified IP address and port.</p> <ul style="list-style-type: none"> Control is enabled by default.
Step 4	<pre>exit</pre> <p>Example: Router(config)# exit </p>	<p>(Optional) Exits global configuration mode and returns to privileged EXEC mode.</p>

Configuring and Scheduling a TCP Connect Operation on the Source Device

Perform only one of the following tasks:

- [Configuring and Scheduling a Basic TCP Connect Operation on the Source Device, page 4](#) (required)
- [Configuring and Scheduling a TCP Connect Operation with Optional Parameters on the Source Device, page 6](#) (required)

Prerequisites

If you are using the IP SLAs Responder, complete the “[Configuring the IP SLAs Responder on the Destination Device](#)” section on [page 3](#) before you start this task.

Configuring and Scheduling a Basic TCP Connect Operation on the Source Device

Restrictions

If an IP SLAs Responder is permanently enabled on the destination IP Address and port, use the **control disable** keywords with the **tcp-connect** command to disable control messages.

SUMMARY STEPS

- enable**
- configure terminal**
- ip sla** *operation-number*
- tcp-connect** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}]
- frequency** *seconds*

EFT REVIEW DRAFT – CISCO CONFIDENTIAL

6. **exit**
7. **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm[:ss]* [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>ip sla <i>operation-number</i></p> <p>Example: Router(config)# ip sla 10</p>	<p>Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.</p>
Step 4	<p>tcp-connect {<i>destination-ip-address</i> <i>destination-hostname</i>} <i>destination-port</i> [source-ip {<i>ip-address</i> <i>hostname</i>} source-port <i>port-number</i>] [control {enable disable}]</p> <p>Example: Router(config-ip-sla)# tcp-connect 172.29.139.132 5000</p>	<p>Defines a TCP Connect operation and enters IP SLA TCP configuration mode.</p> <ul style="list-style-type: none"> • Use the control disable keyword combination only if you disable the IP SLAs control protocol on both the source and target routers.
Step 5	<p>frequency <i>seconds</i></p> <p>Example: Router(config-ip-sla-tcp)# frequency 30</p>	<p>(Optional) Sets the rate at which a specified IP SLAs operation repeats.</p>
Step 6	<p>exit</p> <p>Example: Router(config-ip-sla-tcp)# exit</p>	<p>Exits IP SLA TCP configuration mode and returns to global configuration mode.</p>
Step 7	<p>ip sla schedule <i>operation-number</i> [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>Example: Router(config)# ip sla schedule 10 start-time now life forever</p>	<p>Configures the scheduling parameters for an individual IP SLAs operation.</p>
Step 8	<p>exit</p> <p>Example: Router(config)# exit</p>	<p>(Optional) Exits the global configuration mode and returns to privileged EXEC mode.</p>

EFT REVIEW DRAFT – CISCO CONFIDENTIAL**Examples**

The following example shows the configuration of an IP SLAs operation type of TCP Connect that will start immediately and run indefinitely.

```
ip sla 9
  tcp-connect 172.29.139.132 5000
  frequency 10
!
ip sla schedule 9 life forever start-time now
```

What to Do Next

To view and interpret the results of an IP SLAs operation use the **show ip sla statistics** command. Checking the output for fields that correspond to criteria in your service level agreement will help you determine whether the service metrics are acceptable.

Configuring and Scheduling a TCP Connect Operation with Optional Parameters on the Source Device**Restrictions**

If an IP SLAs Responder is permanently enabled on the destination IP Address and port, use the **control disable** keywords with the **tcp-connect** command to disable control messages.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **tcp-connect** { *destination-ip-address* | *destination-hostname* } *destination-port* [**source-ip** { *ip-address* | *hostname* } **source-port** *port-number*] [**control** { **enable** | **disable**}]
5. **history buckets-kept** *size*
6. **history distributions-of-statistics-kept** *size*
7. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
8. **history filter** { **none** | **all** | **overThreshold** | **failures** }
9. **frequency** *seconds*
10. **history hours-of-statistics-kept** *hours*
11. **history lives-kept** *lives*
12. **owner** *owner-id*
13. **history statistics-distribution-interval** *milliseconds*
14. **tag** *text*
15. **threshold** *milliseconds*
16. **timeout** *milliseconds*
17. **tos** *number*
or
traffic-class *number*

EFT REVIEW DRAFT – CISCO CONFIDENTIAL

18. **flow-label** *number*
19. **exit**
20. **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm[:ss]* [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]
21. **exit**
22. **show ip sla configuration** [*operation-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip sla <i>operation-number</i> Example: Router(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	tcp-connect { <i>destination-ip-address</i> <i>destination-hostname</i> } <i>destination-port</i> [source-ip { <i>ip-address</i> <i>hostname</i> } source-port <i>port-number</i>] [control { enable disable }] Example: Router(config-ip-sla)# tcp-connect 172.29.139.132 5000	Defines a TCP Connect operation and enters IP SLA TCP configuration mode. <ul style="list-style-type: none">• Use the control disable keyword combination only if you disable the IP SLAs control protocol on both the source and target routers.
Step 5	history buckets-kept <i>size</i> Example: Router(config-ip-sla-tcp)# history buckets-kept 25	(Optional) Sets the number of history buckets that are kept during the lifetime of an IP SLAs operation.
Step 6	history distributions-of-statistics-kept <i>size</i> Example: Router(config-ip-sla-tcp)# history distributions-of-statistics-kept 5	(Optional) Sets the number of statistics distributions kept per hop during an IP SLAs operation.
Step 7	history enhanced [interval <i>seconds</i>] [buckets <i>number-of-buckets</i>] Example: Router(config-ip-sla-tcp)# history enhanced interval 900 buckets 100	(Optional) Enables enhanced history gathering for an IP SLAs operation.

EFT REVIEW DRAFT – CISCO CONFIDENTIAL

	Command or Action	Purpose
Step 8	<p>history filter {none all overThreshold failures}</p> <p>Example: Router(config-ip-sla-tcp)# history filter failures</p>	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.
Step 9	<p>frequency seconds</p> <p>Example: Router(config-ip-sla-tcp)# frequency 30</p>	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 10	<p>history hours-of-statistics-kept hours</p> <p>Example: Router(config-ip-sla-tcp)# history hours-of-statistics-kept 4</p>	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 11	<p>history lives-kept lives</p> <p>Example: Router(config-ip-sla-tcp)# history lives-kept 5</p>	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	<p>owner owner-id</p> <p>Example: Router(config-ip-sla-tcp)# owner admin</p>	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13	<p>history statistics-distribution-interval milliseconds</p> <p>Example: Router(config-ip-sla-tcp)# history statistics-distribution-interval 10</p>	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 14	<p>tag text</p> <p>Example: Router(config-ip-sla-tcp)# tag TelnetPollServer1</p>	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 15	<p>threshold milliseconds</p> <p>Example: Router(config-ip-sla-tcp)# threshold 10000</p>	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 16	<p>timeout milliseconds</p> <p>Example: Router(config-ip-sla-tcp)# timeout 10000</p>	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.

EFT REVIEW DRAFT – CISCO CONFIDENTIAL

	Command or Action	Purpose
Step 17	<p>tos <i>number</i></p> <p>or</p> <p>traffic-class <i>number</i></p> <p>Example: Router(config-ip-sla-jitter)# tos 160 or Router(config-ip-sla-jitter)# traffic-class 160</p>	<p>(Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation.</p> <p>or</p> <p>(Optional) In an IPv6 network only, defines the traffic class byte in the IPv6 header for a supported IP SLAs operation.</p>
Step 18	<p>flow-label <i>number</i></p> <p>Example: Router(config-ip-sla-tcp)# flow-label 112233</p>	<p>(Optional) In an IPv6 network only, defines the flow label field in the IPv6 header for a supported IP SLAs operation.</p>
Step 19	<p>exit</p> <p>Example: Router(config-ip-sla-tcp)# exit</p>	<p>Exits TCP configuration submode and returns to global configuration mode.</p>
Step 20	<p>ip sla schedule <i>operation-number</i> [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>Example: Router(config)# ip sla schedule 10 start-time now life forever</p>	<p>Configures the scheduling parameters for an individual IP SLAs operation.</p>
Step 21	<p>exit</p> <p>Example: Router(config)# exit</p>	<p>(Optional) Exits global configuration mode and returns to privileged EXEC mode.</p>
Step 22	<p>show ip sla configuration [<i>operation-number</i>]</p> <p>Example: Router# show ip sla configuration 10</p>	<p>(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.</p>

Examples

The following sample output shows the configuration of all the IP SLAs parameters (including defaults) for the TCP Connect operation number 9.

```

Router# show ip sla configuration 9

Complete Configuration Table (includes defaults)
Entry Number: 9
Owner:
Tag: SL-SGU
Type of Operation to Perform: tcpConnect
Reaction and History Threshold (milliseconds): 5000
Operation Frequency (seconds): 20
Operation Timeout (milliseconds): 60000
Verify Data: FALSE
Status of Entry (SNMP RowStatus): active
    
```

EFT REVIEW DRAFT – CISCO CONFIDENTIAL

```

Protocol Type: ipTcpConn
Target Address: 172.29.139.132
Source Address: 0.0.0.0
Target Port: 5000
Source Port: 0
Request Size (ARR data portion): 1
Response Size (ARR data portion): 1
Control Packets: enabled
Loose Source Routing: disabled
LSR Path:
Type of Service Parameters: 128
Life (seconds): infinite - runs forever
Next Scheduled Start Time: Start Time already passed
Entry Ageout (seconds): never
Connection Loss Reaction Enabled: FALSE
Timeout Reaction Enabled: FALSE
Threshold Reaction Type: never
Threshold Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Reaction Type: none
Verify Error Reaction Enabled: FALSE
Number of Statistic Hours kept: 2
Number of Statistic Paths kept: 1
Number of Statistic Hops kept: 1
Number of Statistic Distribution Buckets kept: 1
Statistic Distribution Interval (milliseconds): 20
Number of History Lives kept: 0
Number of History Buckets kept: 15
Number of History Samples kept: 1
History Filter Type: none

```

Troubleshooting Tips

Use the **debug ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an IP SLAs operation.

What to Do Next

To view and interpret the results of an IP SLAs operation use the **show ip sla statistics** command. Checking the output for fields that correspond to criteria in your service level agreement will help you determine whether the service metrics are acceptable.

Configuration Examples for the IP SLAs TCP Connect Operation

- [Example: Configuring a TCP Connect Operation](#), page 10

Example: Configuring a TCP Connect Operation:

The following example shows how to configure a TCP Connect operation as shown in [Figure 1](#) from Router B to the Telnet port (TCP port 23) of IP Host 1 (IP address 10.0.0.1). The operation is scheduled to start immediately. In this example, the control protocol is disabled on source (Router B). IP SLAs uses the control protocol to notify the IP SLAs Responder to enable the target port temporarily. This action allows the Responder to reply to the TCP Connect operation. In this example, because the target is not a router and a well-known TCP port is used, there is no need to send the control message.

EFT REVIEW DRAFT – CISCO CONFIDENTIAL**Router A Configuration**

```
configure terminal
ip sla responder tcp-connect ipaddress 10.0.0.1 port 23
```

Router B Configuration

```
ip sla 9
tcp-connect 10.0.0.1 23 control disable
frequency 30
tos 128
timeout 1000
tag FLL-RO
ip sla schedule 9 start-time now
```

The following example shows how to configure a TCP Connect operation with a specific port, port 23, and without an IP SLAs Responder. The operation is scheduled to start immediately and run indefinitely.

```
ip sla 9
tcp-connect 173.29.139.132 21 control disable
frequency 30
ip sla schedule 9 life forever start-time now
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS IP SLAs commands	Cisco IOS IP SLAs Command Reference

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> CISCO-RTTMON-MIB IPV6-FLOW-LABEL-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>

EFT REVIEW DRAFT – CISCO CONFIDENTIAL**RFCs**

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

EFT REVIEW DRAFT – CISCO CONFIDENTIAL

Feature Information for the IP SLAs TCP Connect Operation

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for the IP SLAs TCP Connect Operation

Feature Name	Releases	Feature Information
IP SLAs TCP Connect Operation	12.2(31)SB2 12.2(33)SRB1 12.2(33)SXH 12.2(32)SY 12.3(14)T 15.0(1)S Cisco IOS XE 3.1.0SG	The Cisco IOS IP SLAs Transmission Control Protocol (TCP) connect operation allows you to measure the network response time taken to perform a TCP Connect operation between a Cisco device and other devices using IP.
IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	12.2(33)SRC 12.2(33)SB 12.4(20)T Cisco IOS XE 3.1.0SG 12.2(50)SY	Support was added for operability in IPv6 networks.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006-2011 Cisco Systems, Inc. All rights reserved.

EFT REVIEW DRAFT – CISCO CONFIDENTIAL