



Configuring IP SLAs TCP Connect Operations

This module describes how to configure an 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, page 1](#)
- [Information About the IP SLAs TCP Connect Operation, page 2](#)
- [How to Configure the IP SLAs TCP Connect Operation, page 3](#)
- [Configuration Examples for IP SLAs TCP Connect Operations, page 10](#)
- [Additional References, page 10](#)
- [Feature Information for the IP SLAs TCP Connect Operation, page 11](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 table.

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

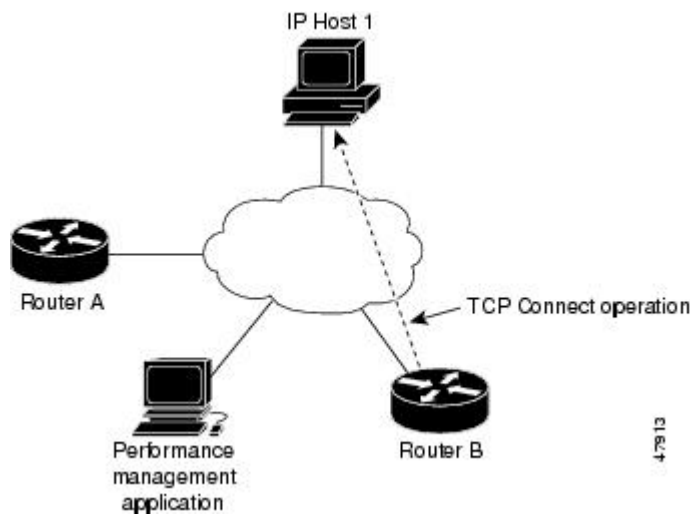
Information About the IP SLAs TCP Connect Operation

TCP Connect Operation

The IP SLAs TCP Connect operation measures the response time taken to perform a TCP Connect operation between a Cisco device 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 the figure below Device 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 Device 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 device is a Cisco device, 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.

How to Configure the IP SLAs TCP Connect Operation

Configuring the IP SLAs Responder on the Destination Device

Before You Begin

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. Do one of the following:
 - **ip sla responder**
 - **ip sla responder tcp-connect** *ipaddress ip-address port port*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	Do one of the following: <ul style="list-style-type: none">• ip sla responder• ip sla responder tcp-connect <i>ipaddress ip-address port port</i> Example: Device(config)# ip sla responder	(Optional) Temporarily enables IP SLAs responder functionality on the Cisco device in response to control messages from source. or (Optional) Required only if protocol control is explicitly disabled on the source device. Permanently enables IP SLAs responder functionality on the specified IP address and port. <ul style="list-style-type: none">• Control is enabled by default.

	Command or Action	Purpose
	Example: <pre>Device(config)# ip sla responder tcp-connect ipaddress 172.29.139.132 port 5000</pre>	
Step 4	exit Example: <pre>Device(config)# exit</pre>	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Configuring and Scheduling a TCP Connect Operation on the Source Device

Perform only one of the following tasks:

Prerequisites

If you are using the IP SLAs Responder, complete the "Configuring the IP SLAs Responder on the Destination Device" section before you start this task.

Configuring a Basic TCP Connect Operation on the Source Device

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. **frequency** *seconds*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla operation-number Example: Device(config)# ip sla 10	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 4	tcp-connect {destination-ip-address destination-hostname} destination-port [source-ip {ip-address hostname} source-port port-number] [control {enable disable}] Example: Device(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 devices.
Step 5	frequency seconds Example: Device(config-ip-sla-tcp)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 6	end Example: Device(config-ip-sla-tcp)# end	Returns to global configuration mode.

Troubleshooting Tips

- If the IP SLAs operation is not running and not generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When data verification is 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 ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an IP SLAs operation.

What to Do Next

To add proactive threshold conditions and reactive triggering for generating traps (or for starting another operation) to an IP SLAs operation, see the “Configuring Proactive Threshold Monitoring” section.

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

Configuring a TCP Connect Operation with Optional Parameters on the Source Device

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. Do one of the following:
 - **tos** *number*
 - **traffic-class** *number*
18. **flow-label** *number*
19. **exit**
20. **show ip sla configuration** [*operation-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip sla <i>operation-number</i> Example: Device(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: Device(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 devices.
Step 5	history buckets-kept <i>size</i> Example: Device(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: Device(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 [<i>interval seconds</i>] [<i>buckets number-of-buckets</i>] Example: Device(config-ip-sla-tcp)# history enhanced interval 900 buckets 100	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 8	history filter { none all overThreshold failures } Example: Device(config-ip-sla-tcp)# history filter failures	(Optional) Defines the type of information kept in the history table for an IP SLAs operation.

	Command or Action	Purpose
Step 9	frequency <i>seconds</i> Example: Device(config-ip-sla-tcp)# frequency 30	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 10	history hours-of-statistics-kept <i>hours</i> Example: Device(config-ip-sla-tcp)# history hours-of-statistics-kept 4	(Optional) Sets the number of hours for which statistics are maintained for an IP SLAs operation.
Step 11	history lives-kept <i>lives</i> Example: Device(config-ip-sla-tcp)# history lives-kept 2	(Optional) Sets the number of lives maintained in the history table for an IP SLAs operation.
Step 12	owner <i>owner-id</i> Example: Device(config-ip-sla-tcp)# owner admin	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.
Step 13	history statistics-distribution-interval <i>milliseconds</i> Example: Device(config-ip-sla-tcp)# history statistics-distribution-interval 10	(Optional) Sets the time interval for each statistics distribution kept for an IP SLAs operation.
Step 14	tag <i>text</i> Example: Device(config-ip-sla-tcp)# tag TelnetPollServer1	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 15	threshold <i>milliseconds</i> Example: Device(config-ip-sla-tcp)# threshold 10000	(Optional) Sets the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation.
Step 16	timeout <i>milliseconds</i> Example: Device(config-ip-sla-tcp)# timeout 10000	(Optional) Sets the amount of time an IP SLAs operation waits for a response from its request packet.
Step 17	Do one of the following: <ul style="list-style-type: none"> • tos <i>number</i> • traffic-class <i>number</i> 	(Optional) For IPv4: Defines the ToS byte in the IPv4 header of an IP SLAs operation. or (Optional) For IPv6: Defines the traffic class byte in the IPv6 header for a supported IP SLAs operation.

	Command or Action	Purpose
	Example: Device(config-ip-sla-jitter)# tos 160 Example: Device(config-ip-sla-jitter)# traffic-class 160	
Step 18	flow-label <i>number</i> Example: Device(config-ip-sla-tcp)# flow-label 112233	(Optional) For IPv6: Defines the flow label field in the IPv6 header for a supported IP SLAs operation.
Step 19	exit Example: Device(config-ip-sla-tcp)# exit	Exits TCP configuration submode and returns to global configuration mode.
Step 20	show ip sla configuration [<i>operation-number</i>] Example: Device# show ip sla configuration 10	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

Troubleshooting Tips

- If the IP SLAs operation is not running and not generating statistics, add the **verify-data** command to the configuration of the operation (while configuring in IP SLA configuration mode) to enable data verification. When data verification is 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 ip sla trace** and **debug ip sla error** commands to help troubleshoot issues with an IP SLAs operation.

What to Do Next

To add proactive threshold conditions and reactive triggering for generating traps (or for starting another operation) to an IP SLAs operation, see the “Configuring Proactive Threshold Monitoring” section.

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

Configuration Examples for IP SLAs TCP Connect Operations

Example Configuring a TCP Connect Operation

The following example shows how to configure a TCP Connect operation from Device B to the Telnet port (TCP port 23) of IP Host 1 (IP address 10.0.0.1), as shown in the "TCP Connect Operation" figure in the "Information About the IP SLAs TCP Connect Operation" section. The operation is scheduled to start immediately. In this example, the control protocol is disabled on the source (Device 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 Cisco device and a well-known TCP port is used, there is no need to send the control message.

Device A (target device) Configuration

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

Device B (source device) 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	<i>Cisco IOS IP SLAs Command Reference</i>

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
CISCO-RTTMON-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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

Feature Information for the IP SLAs TCP Connect Operation

The following table provides release information about the feature or features described in this module. This table 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.

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

Table 1: Feature Information for the IP SLAs TCP Connect Operation

Feature Name	Releases	Feature Information
IP SLAs TCP Connect Operation		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)		Support was added for operability in IPv6 networks.
IP SLAs VRF Aware 2.0		Support was added for IP SLAs VRF-aware capabilities for TCP connect, FTP, HTTP and DNS client operation types.