Configuring IP SLAs TCP Connect Operations

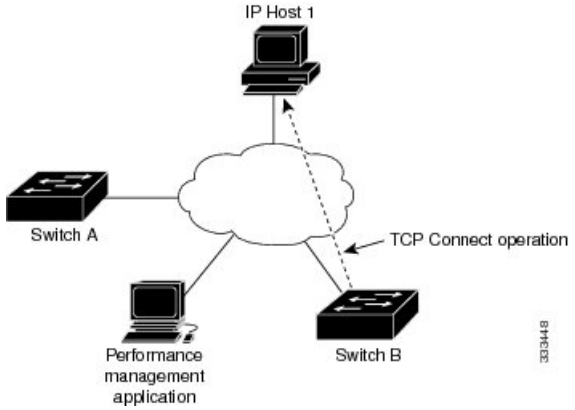
This chapter describes how to configure an IP Service Level Agreements (SLAs) TCP Connect operation to measure the response time taken to perform a TCP Connect operation between a Cisco switch and devices using IPv4. TCP Connect accuracy is enhanced by using the IP SLAs Responder at the destination Cisco switch. This chapter also describes 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.

This chapter includes these sections.

Information About the TCP Connect Operation

The IP SLAs TCP Connect operation measures the response time that is taken to perform a TCP Connect operation between a Cisco switch 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 following figure, Switch B is configured as the source IP SLAs device and a TCP Connect operation is configured with the destination device as IP Host 1.



The connection response time is computed by measuring the time that is taken between sending a TCP request message from Switch 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 switch is a Cisco switch, the IP SLAs Responder 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 connections to help you verify your IP service levels.

Guidelines and Limitations for Configuring IP SLAs TCP Connect Operations

- **show** commands with the **internal** keyword are not supported.

Configuring CoPP for IP SLA Packets

When using IP SLA operations on a large scale, a specific CoPP configuration to allow the IP SLA packets to pass through might be needed. Because IP SLA uses user-defined UDP ports, there is no way to allow all IP SLA packets to the control plane. However, you can specify each destination/source port that IP SLA can use.

For more information about the verified scalability of the number of IP SLA probes, see the *Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*.

The following CoPP configuration example allows IP SLA packets to pass through. It assumes destination ports and source ports in the range of 6500-7000. In this example, if “insert-before” is not specified, "copp-ipsla" will be added after “class-default.”

Note The following configuration example might vary based on platform/hardware type. Please refer to the Cisco Nexus 9000 Series NX-OS Security Configuration Guide for details about configuring IP ACL and CoPP.

```
ip access-list acl-sla-allow
  10 remark ### ALLOW SLA control packets from 1.1.1.0/24
  20 permit udp 1.1.1.0/24 any eq 1967
  30 remark ### ALLOW SLA data packets from 1.1.1.0/24 using ports 6500-7000
  40 permit udp 1.1.1.0/24 any range 6500 7000

class-map type control-plane match-any copp-ipsla
  match access-group name acl-sla-allow

policy-map type control-plane Custom-copp-policy-strict
    class copp-ipsla insert-before Custom-copp-class-l2-default
    police cir 1500 kbps

control-plane
  service-policy input Custom-copp-policy-strict

switch# show policy-map interface control-plane | be copp-ipsla
    class-map copp-ipsla (match-any)
      match access-group name acl-sla-allow
      set cos 7
      police cir 1500 kbps , bc 32000 bytes
      module 1 :
        transmitted 0 bytes;
        dropped 0 bytes;

    class-map Custom-copp-class-l2-default (match-any)
      match access-group name Custom-copp-acl-mac-undesirable
      set cos 0
      police cir 400 kbps , bc 32000 bytes
      module 1 :
        transmitted 0 bytes;
        dropped 0 bytes;

    class-map class-default (match-any)
      set cos 0
      police cir 400 kbps , bc 32000 bytes
      module 1 :
        transmitted 122 bytes;
        dropped 0 bytes;
```

Matching the Netstack Port Range

IP SLA only accepts ports within the local netstack port range. The source and destination ports used in the probe's configuration must match the supported netstack ports on the SLA sender and the SLA responder.

When performing ISSU from earlier versions to version 9.3(1) and later versions, ensure that the features with user-defined ports, such as SSH port, are within the range mentioned in the following table.

Table 1: Port Range for ISSU

Version	Default port-range
9.3(1)	Kstack local port range (15001 - 58000) Netstack local port range (58001 - 63535) nat port range (63536 - 65535)
9.3(2)	Kstack local port range (15001 - 58000) Netstack local port range (58001 - 63535) nat port range (63536 - 65535)
9.3(3) onwards	Kstack local port range (15001 - 58000) Netstack local port range (58001 - 60535) nat port range (60536 - 65535)

You can use the **show sockets local-port-range** command to view the port range on the sender/responder.

The following is an example of viewing the netstack port range:

```
switch# show sockets local-port-range

Kstack local port range (15001 - 22002)
Netstack local port range (22003 - 65535)
```

Configuring the IP SLAs Responder on the Destination Device

This section describes how to configure 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. **feature sla responder**
4. Do one of the following:
   - **ip sla responder**

     Example:

     ```
     switch(config)# ip sla responder
     ```
   - **ip sla responder tcp-connect ipaddress** *ip-address* **port** *port*

     Example:

```
switch(config)# ip sla responder tcp-connect ipaddress 172.29.139.132 port 5000
```

5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `switch# configure terminal`	Enters global configuration mode.
Step 3	**feature sla responder** **Example:** `switch(config)# feature sla responder`	Enables the IP SLAs responder feature.

Step 4	Do one of the following:
	• **ip sla responder**
	Example:
	`switch(config)# ip sla responder`
	• **ip sla responder tcp-connect ipaddress** *ip-address* **port** *port*
	Example:
	`switch(config)# ip sla responder tcp-connect ipaddress 172.29.139.132 port 5000`
		-
		• (Optional) Temporarily enables IP SLAs Responder functionality on a Cisco device in response to control messages from a source.
		• (Optional) Required only if protocol control is disabled on the source. The command permanently enables the IP SLAs Responder functionality on a specified IP address and port.
		Control is enabled by default.

Step 5	**exit** **Example:** `switch(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Configuring and Scheduling a TCP Connect Operation on the Source Device

This section describes how to configure and schedule a TCP connect operation on the source device.

Perform only one of the following tasks to configure and schedule a TCP connect operation on the source device:

- Configuring and scheduling a basic TCP connect operation on the source device

- Configuring and scheduling a TCP connect operation with optional parameters on the source device

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

This section describes how to configure and schedule a basic TCP connect operation on a source device.

Note 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.

Tip

- If the IP SLAs operation is not running and 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 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 sender trace** and **debug ip sla sender error** commands to help troubleshoot issues with an IP SLAs operation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **feature sla sender**
4. **ip sla** *operation-number*
5. **tcp-connect** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port***port-number*] [**control** {**enable** | **disable**}]
6. **frequency** *seconds*
7. **exit**
8. **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*monthday* | *daymonth*] | **pending** | **now** | **after** *hh*:*mm*:*ss*] [**ageout** *seconds*] [**recurring**]
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal`	
Step 3	**feature sla sender** **Example:** `switch(config)# feature sla sender`	Enables the IP SLAs operation feature.
Step 4	**ip sla** *operation-number* **Example:** `switch(config)# ip sla 10`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 5	**tcp-connect** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port***port-number*] [**control** {**enable** | **disable**}] **Example:** `switch(config-ip-sla)# tcp-connect 172.29.139.132 5000`	Defines a TCP Connect operation and enters IP SLA TCP configuration mode. Use the **control disable** keyword combination only if you disable the IP SLAs control protocol on both the source and target switches.
Step 6	**frequency** *seconds* **Example:** `switch(config-ip-sla-tcp)# frequency 60`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 7	**exit** **Example:** `switch(config-ip-sla-tcp)# exit`	Exits IP SLA TCP configuration mode and returns to global configuration mode.
Step 8	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*monthday* | *daymonth*] | **pending** | **now** | **after** *hh*:*mm*:*ss*] [**ageout** *seconds*] [**recurring**] **Example:** `switch(config)# ip sla schedule 10 start-time now life forever`	Configures the scheduling parameters for an individual IP SLAs operation.
Step 9	**exit** **Example:** `switch(config)# exit`	(Optional) Exits the global configuration mode and returns to privileged EXEC mode.

Example

This example shows how to configure an IP SLAs operation type of TCP Connect that will start immediately and run indefinitely:

```
feature sla sender
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 add proactive threshold conditions and reactive triggering for generating traps or for starting another operation, see the "Configuring Proactive Threshold Monitoring" section.

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 helps you to determine whether the service metrics are acceptable.

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

This section describes how to configure and schedule a TCP connect operation with optional parameters on a source device.

Note 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.

Tip

- If the IP SLAs operation is not running and 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 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **feature sla sender**
4. **ip sla** *operation-number*

5. **tcp-connect** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}]
6. **history buckets-kept** *size*
7. **history distributions-of-statistics-kept** *size*
8. **history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*]
9. **history filter** {**none** | **all** | **overThreshold** | **failures**}
10. **frequency** *seconds*
11. **history hours-of-statistics-kept** *hours*
12. **history lives-kept** *lives*
13. **owner** *owner-id*
14. **history statistics-distribution-interval** *milliseconds*
15. **tag** *text*
16. **threshold** *milliseconds*
17. **timeout** *milliseconds*
18. **tos** *number*
19. **exit**
20. **ip sla schedule** *operation-number* [**life** {**forever**| *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*monthday* | *daymonth*] | **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:** `switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `switch# configure terminal`	Enters global configuration mode.
Step 3	**feature sla sender** **Example:** `switch(config)# feature sla sender`	Enables the IP SLAs operation feature.
Step 4	**ip sla** *operation-number* **Example:** `switch(config)# ip sla 10`	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
Step 5	**tcp-connect** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*} **source-port** *port-number*] [**control** {**enable** | **disable**}]	Defines a TCP Connect operation and enters IP SLA TCP configuration mode.

	Command or Action	Purpose
	Example: `switch(config-ip-sla)# tcp-connect 172.29.139.132 5000`	Use the **control disable** keyword combination only if you disable the IP SLAs control protocol on both the source and target switches.
Step 6	**history buckets-kept** *size* **Example:** `switch(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 7	**history distributions-of-statistics-kept** *size* **Example:** `switch(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 8	**history enhanced** [**interval** *seconds*] [**buckets** *number-of-buckets*] **Example:** `switch(config-ip-sla-tcp)# history enhanced interval 900 buckets 100`	(Optional) Enables enhanced history gathering for an IP SLAs operation.
Step 9	**history filter** {**none** | **all** | **overThreshold** | **failures**} **Example:** `switch(config-ip-sla-tcp)# history filter failures`	(Optional) Defines the type of information that is kept in the history table for an IP SLAs operation.
Step 10	**frequency** *seconds* **Example:** `switch(config-ip-sla-tcp)# frequency 60`	(Optional) Sets the rate at which a specified IP SLAs operation repeats.
Step 11	**history hours-of-statistics-kept** *hours* **Example:** `switch(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 12	**history lives-kept** *lives* **Example:** `switch(config-ip-sla-tcp)# history lives-kept 5`	(Optional) Sets the number of lives that are maintained in the history table for an IP SLAs operation.
Step 13	**owner** *owner-id* **Example:** `switch(config-ip-sla-tcp)# owner admin`	(Optional) Configures the Simple Network Management Protocol (SNMP) owner of an IP SLAs operation.

	Command or Action	Purpose
Step 14	**history statistics-distribution-interval** *milliseconds* **Example:** `switch(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 15	**tag** *text* **Example:** `switch(config-ip-sla-tcp)# tag TelnetPollServer1`	(Optional) Creates a user-specified identifier for an IP SLAs operation.
Step 16	**threshold** *milliseconds* **Example:** `switch(config-ip-sla-tcp)# threshold 10000`	(Optional) Sets the upper threshold value for calculating network monitoring statistics that are created by an IP SLAs operation.
Step 17	**timeout** *milliseconds* **Example:** `switch(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 18	**tos** *number* **Example:** `switch(config-ip-sla-jitter)# tos 160` **Example:**	(Optional) In an IPv4 network only, defines the ToS byte in the IPv4 header of an IP SLAs operation.
Step 19	**exit** **Example:** `switch(config-ip-sla-tcp)# exit`	Exits TCP configuration submode and returns to global configuration mode.
Step 20	**ip sla schedule** *operation-number* [**life** {**forever**| *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*monthday* | *daymonth*] | **pending** | **now** | **after** *hh*:*mm*:*ss*] [**ageout** *seconds*] [**recurring**] **Example:** `switch(config)# ip sla schedule 10 start-time now life forever`	Configures the scheduling parameters for an individual IP SLAs operation.
Step 21	**exit** **Example:** `switch(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 22	**show ip sla configuration** [*operation-number*] **Example:** `switch# show ip sla configuration 10`	(Optional) Displays configuration values including all defaults for all IP SLAs operations or a specified operation.

Example

This example shows how to configure all the IP SLAs parameters (including defaults) for the TCP Connect operation number 10:

```
switch# show ip sla configuration 10
IP SLAs Infrastructure Engine-III
Entry number: 10
Owner: admin
Tag: TelnetPollServer1
Operation timeout (milliseconds): 10000
Type of operation to perform: tcp-connect
Target address/Source address: 101.101.101.1/0.0.0.0
Target port/Source port: 5000/0
Type Of Service parameter: 0xa0
Vrf Name: default
Control Packets: enabled
Schedule:
   Operation frequency (seconds): 60  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 10000
Distribution Statistics:
   Number of statistic hours kept: 4
   Number of statistic distribution buckets kept: 5
   Statistic distribution interval (milliseconds): 10
Enhanced History:
   Aggregation Interval:900 Buckets: 100
History Statistics:
   Number of history Lives kept: 0
   Number of history Buckets kept: 25
   History Filter Type: Failures
```

What to do next

To add proactive threshold conditions and reactive triggering for generating traps or for starting another operation, see the "Configuring Proactive Threshold Monitoring" section.

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 helps you to determine whether the service metrics are acceptable.

Configuration Example for a TCP Connect Operation

This example shows how to configure a TCP Connect operation from Switch 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 (Switch B). IP SLAs use 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 switch and a well-known TCP port is used, there is no need to send the control message.

Switch A Configuration

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

Switch B Configuration

```
configure terminal
 feature sla sender
 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
```

This example shows how to configure a TCP Connect operation with a specific port, port 21, and without an IP SLAs Responder. The operation is scheduled to start immediately and run indefinitely.

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