CHAPTER 41

Configuring Cisco IOS IP SLAs Operations

This chapter describes how to use Cisco IOS IP Service Level Agreements (SLAs) on the Catalyst 3560 switch. Cisco IP SLAs is a part of Cisco IOS software that allows Cisco customers to analyze IP service levels for IP applications and services by using active traffic monitoring—the generation of traffic in a continuous, reliable, and predictable manner—for measuring network performance. With Cisco IOS 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. Cisco IOS IP SLAs can perform network assessments, verify quality of service (QoS), ease the deployment of new services, and assist with network troubleshooting.

Note Switches running the IP base image support only IP SLAs responder functionality and must be configured with another device that supports full IP SLAs functionality, for example, a Catalyst 3560 switch running the IP services image.

For more information about IP SLAs, see the *Cisco IOS IP SLAs Configuration Guide, Release 12.4T* this URL:

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

For command syntax information, see the command reference at this URL:

http://www.cisco.com/en/US/docs/ios/ipsla/command/reference/sla_book.html

This chapter consists of these sections:

Understanding Cisco IOS IP SLAs

Depending on the specific Cisco IOS IP SLAs operation, various network performance statistics are monitored within the Cisco device and stored in both command-line interface (CLI) and Simple Network Management Protocol (SNMP) MIBs. IP SLAs packets have configurable IP and application layer options such as source and destination IP address, User Datagram Protocol (UDP)/TCP port numbers, a type of service (ToS) byte (including Differentiated Services Code Point [DSCP] and IP Prefix bits), Virtual Private Network (VPN) routing/forwarding instance (VRF), and URL web address.

Because Cisco IP SLAs is Layer 2 transport independent, you can configure end-to-end operations over disparate networks to best reflect the metrics that an end user is likely to experience. IP SLAs collects a unique subset of these 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

Because Cisco IOS IP SLAs is SNMP-accessible, it can also be used by performance-monitoring applications like CiscoWorks Internetwork Performance Monitor (IPM) and other third-party Cisco partner performance management products. You can find more details about network management products that use Cisco IOS IP SLAs at this URL:

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

Using IP SLAs can provide these benefits:

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 to verify that the existing QoS is sufficient for new IP services.

Edge-to-edge network availability monitoring for proactive verification and connectivity testing of network resources (for example, shows the network availability of an NFS server used to store business critical data from a remote site).

Troubleshooting of network operation by providing consistent, reliable measurement that immediately identifies problems and saves troubleshooting time.

Multiprotocol Label Switching (MPLS) performance monitoring and network verification (if the switch supports MPLS)

This section includes this information about IP SLAs functionality:

Using Cisco IOS IP SLAs to Measure Network Performance, page 41-3

IP SLAs Responder and IP SLAs Control Protocol, page 41-4

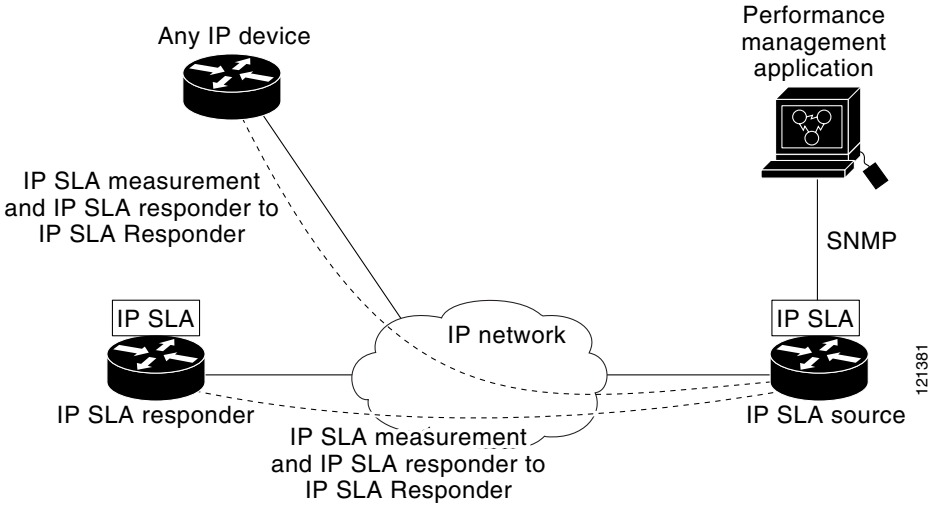
Response Time Computation for IP SLAs, page 41-4

IP SLAs Operation Scheduling, page 41-5

IP SLAs Operation Threshold Monitoring, page 41-5

Using Cisco IOS IP SLAs to Measure Network Performance

Figure 41-1 Cisco IOS IP SLAs Operation



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

1.
2.
3.
4.
5.
6.

Note

show ip sla application privileged EXEC command to verify that the operation type is supported on your software image.

IP SLAs Responder and IP SLAs Control Protocol

Note

Catalyst 2960, or a Cisco ME 2400 or IE 3000 switch, or a Catalyst 3560 or 3750 switch running the IP base image. The responder does not need to support full IP SLAs functionality.

Figure 41-1 shows where the Cisco IOS IP SLAs responder fits in the IP network. The responder listens on a specific port for control protocol messages sent by an IP SLAs operation. Upon receipt of the control message, it enables the specified UDP or TCP port for the specified duration. During this time, the responder accepts the requests and responds to them. It disables the port after it responds to the IP SLAs packet, or when the specified time expires. MD5 authentication for control messages is available for added security.

You do not need to enable the responder on the destination device for all IP SLAs operations. For example, a responder is not required for services that are already provided by the destination router (such as Telnet or HTTP). You cannot configure the IP SLAs responder on non-Cisco devices and Cisco IOS IP SLAs can send operational packets only to services native to those devices.

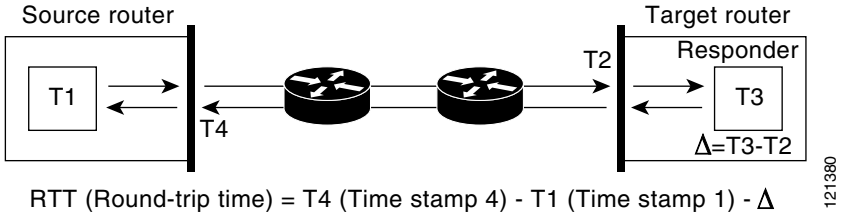
Response Time Computation for IP SLAs

Switches and routers can take tens of milliseconds to process incoming packets due to other high priority processes. This delay affects the response times because the test-packet reply might be in a queue while waiting to be processed. In this situation, the response times would not accurately represent true network delays. IP SLAs minimizes these processing delays on the source device as well as on the target device (if the responder is being used) to determine true round-trip times. IP SLAs test packets use time stamping to minimize the processing delays.

When the IP SLAs responder is enabled, it allows the target device to take time stamps 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-milliseconds (ms).

Figure 41-2 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 41-2 Cisco IOS IP SLAs Responder Time Stamping



IP SLAs Operation Scheduling

an IP SLAs operation, you must schedule the operation to begin capturing statistics and collecting error information. You can schedule an operation to start immediately or to start at a certain month, day, and hour. You can use the *pending* option to set the operation to start at a later time. The pending option is an internal state of the operation that is visible through SNMP. The pending state is also used when an operation is a reaction (threshold) operation waiting to be triggered. You can schedule a single IP SLAs operation or a group of operations at one time.

You can schedule several IP SLAs operations by using a single command through the Cisco IOS CLI or the CISCO RTTMON-MIB. Scheduling the operations to run at evenly distributed times allows you to control the amount of IP SLAs monitoring traffic. This distribution of IP SLAs operations helps minimize the CPU utilization and thus improves network scalability.

For more details about the IP SLAs multioperations scheduling functionality, see the "IP SLAs—Multiple Operation Scheduling" chapter of the at this URL:

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

To support successful service level agreement monitoring, you must have mechanisms that notify you immediately of any possible violation. IP SLAs can send SNMP traps that are triggered by events such as these:

- Connection loss
- Timeout
- Round-trip time threshold
- Average jitter threshold
- One-way packet loss
- One-way jitter

Configuration Guide at this URL:

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/12_4t/sla_12_4t_book.html

Configuring IP SLAs Operations

Note

-
-
- , page 41-8
- Analyzing IP Service Levels by Using the UDP Jitter Operation, page 41-8
- Analyzing IP Service Levels by Using the ICMP Echo Operation, page 41-11

Default Configuration

Configuration Guidelines

Cisco IOS IP SLAs Command Reference, Release 12.4T

```
Switch# show ip sla application
        IP SLAs
Version: 2.2.0 Round Trip Time MIB, Infrastructure Engine-II
Time of last change in whole IP SLAs: 22:17:39.117 UTC Fri Jun
Estimated system max number of entries: 15801

Estimated number of configurable operations: 15801
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0

        Supported Operation Types
Type of Operation to Perform: 802.1agEcho
Type of Operation to Perform: 802.1agJitter
Type of Operation to Perform: dhcp
Type of Operation to Perform: dns
Type of Operation to Perform: echo
Type of Operation to Perform: ftp
Type of Operation to Perform: http
Type of Operation to Perform: jitter
Type of Operation to Perform: pathEcho
Type of Operation to Perform: pathJitter
Type of Operation to Perform: tcpConnect
Type of Operation to Perform: udpEcho

IP SLAs low memory water mark: 21741224
```

	Command	Purpose
Step 1	**configure terminal**	
	ip sla responder {**tcp-connect** | } *ip-address* *port-number*	*ip-address* *port-number*
	copy running-config startup-config	

no ip sla responder

```
Switch(config)# ip sla responder udp-echo 172.29.139.134 5000
```

Analyzing IP Service Levels by Using the UDP Jitter Operation

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

0

operation-number	

udp-jitter *destination-hostname* *destination-port* *ip-address hostname* *port-number* **enable disable** **num-packets** *number-of-packets* **interval** *interpacket-interval*	*destination-ip-address destination-hostname* *destination-port* *ip-address hostname —* *port-number* *number-of-packets* *inter-packet-interval*
frequency *seconds*	
exit	
ip sla monitor schedule **life forever** **start-time** *month day day month* *hh:mm:ss* *seconds*	*operation-number* *seconds* *hh:mm:ss* *seconds*

	Command	Purpose
Step 7		
Step 8		
Step 9		

operation-number

```
                udp-jitter 172.29.139.134 5000
                       frequency 30
                       exit
              ip sla schedule 5 start-time now life forever
              end
      show ip sla configuration 10
```

```
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

Analyzing IP Service Levels by Using the ICMP Echo Operation

Note

	Command	Purpose
Step 1		
Step 2		
Step 3		• • •
Step 4		
Step 5		
Step 6		• • • • •
Step 7		

	Command	Purpose
Step 8		
Step 9		

Monitoring IP SLAs Operations

Table 41-1 Monitoring IP SLAs Operations

entry-number | |	
collection-statistics | configuration ldp operational-state | scan-queue | summary | neighbors	
show ip sla reaction-configuration	
show ip sla reaction-trigger	
show ip sla responder	
show ip sla statistics aggregated details	