Cisco IOS® IP SLAs Lab Guide
January 2007 – Cisco Networkers Europe

Emmanuel Tychon, <etychon@cisco.com>

Formatted: Italian Italy

Field Code Changed

Formatted: Italian Italy

Deleted: INTRODUCTION 2¶
What is IP SLAs? 2¶
Cisco IOS IP SLAs Responder and IP SLAs Control Protocol 3¶
Response Time Computation for Cisco IOS IP SLAs 4¶
Cisco IOS IP SLAs Operation Thresholds 7¶
PLAYING AROUND 8¶
Lab Topology 8¶
UDP Jitter operation 8¶
UDP Jitter operation for VoIP applications 10¶
IP SLAs multiple operations scheduling 11¶
Using thresholds with IP SLAs operations 12¶
Go a little further 14¶
Documentation 15¶

Introduction

What is IP SLA?

This module describes Cisco IOS IP Service Level Agreements (SLAs). IP SLA is a portfolio of technologies embedded in most devices that run Cisco IOS software which allows Cisco customers to analyze IP service levels for IP applications and services and by doing so increase productivity, lower operational costs, and reduce the frequency of network outages. IP SLA uses active traffic monitoring—the generation of traffic in a continuous, reliable, and predictable manner—for measuring network performance.

By using IP SLAs service providers can measure and provide reporting against service level agreements while 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) Management Information Bases (MIBs).

Cisco IP SLAs simulate network data and IP services and collects network performance information in real time. The information collected includes data about response time, one-way latency, jitter (inter-packet 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 performs 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 SLA operations can be used for troubleshooting, problem analysis, and to assist with designing network topologies.

This table shows some of the various types of IP SLA operations, what each operation measures and for what purpose the operation is used. Most of the operations are described in more detail in the Cisco IOS Documentation.

Deleted: s
Deleted: s
Deleted: y
Deleted: ,
Deleted: , to
Deleted: to
Deleted: to
Deleted: s
Deleted: U
Deleted: s,
Deleted: customer
Deleted: ,
Deleted: and
Deleted: ,
Deleted: s
Deleted: ,
Deleted: It
Deleted: s
Deleted: ,
Deleted: s
Deleted: for
Deleted: for
Deleted: s
Deleted: ,
Deleted: ¶

IP SLAs Operation	Measurements	Key Monitoring Application
UDP Jitter	Measures round-trip delay, one-way delay, one-way jitter, one-way packet loss, and connectivity testing of networks that carry UDP traffic, such as voice. Note One-way delay requires time synchronization between source and target routers.	Voice and data network performance. General IP performance Note: This is the most commonly used IP SLAs operation
ICMP Path Jitter	Measures hop-by-hop jitter, packet loss, and delay measurement statistics in an IP network.	Voice and data network performance General IP performance
UDP Jitter for VoIP	Measures round-trip delay, one-way delay, one-way jitter, and one-way packet loss for VoIP traffic. Codec simulation G.711 u-law, G.711 a-law, and G.729A. MOS and ICPIF voice quality scoring capability. Note One-way delay requires time synchronization between source and target routers.	VoIP network and performance
UDP Echo	Measures round-trip delay of UDP traffic.	Server and IP application performance. Connectivity testing
ICMP Echo	Measures round-trip delay for the full path.	IP performance, Connectivity measurement
ICMP Path Echo	Measures round-trip delay and hop-by-hop round-trip delay.	Connectivity measurement, Identify bottlenecks in the path
HTTP	Measures round-trip time to retrieve a web page.	Web server performance
TCP Connect	Measures the time taken to connect to a target device with TCP.	Server and application performance
FTP	Measures round-trip time to transfer a file.	FTP server performance

Formatted: Font: Bold, Complex Script Font: Bold

Formatted: Left

Formatted Table

Formatted: Left

Formatted: Left

Formatted: Left

Formatted: Left

Formatted: Left

Formatted: Left

Formatted: Left

Formatted: Left

Formatted: Left

Cisco IOS IP SLA Responder and IP SLA Control Protocol

Formatted: Italian Italy

Deleted: s

Deleted: s

The IP SLA 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 SLA Responder provides an enormous advantage with accurate measurements without the need for dedicated probes and additional statistics that are 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 an IP SLA Responder.

Deleted: s

Deleted: s

Deleted: destination

Deleted: s

The IP SLAs Responder listens on a specific port for control protocol messages sent by an IP SLAs operation (see Figure 1 below). 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 the control messages is available.

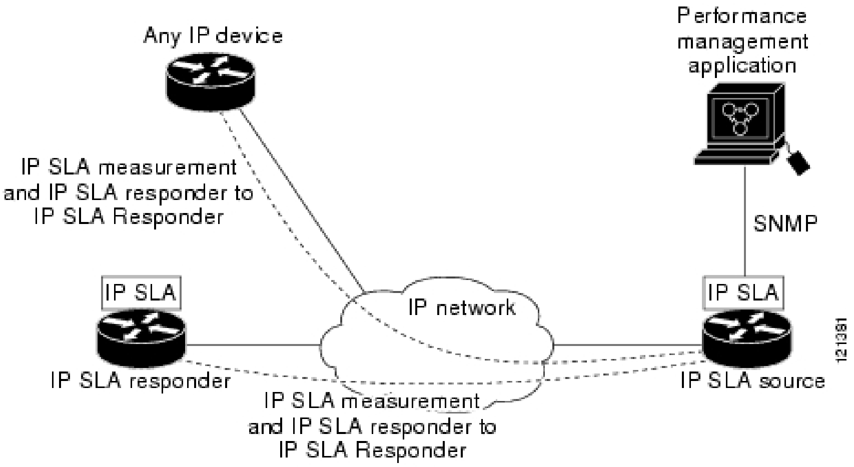
Deleted: Look at the figure below.

Deleted: ,

Deleted: ,

Deleted: ,

Deleted: ,


Any IP device
Performance management application
IP SLA measurement and IP SLA responder to IP SLA Responder
SNMP
IP SLA
IP network
IP SLA
121381
IP SLA responder
IP SLA source
IP SLA measurement and IP SLA responder to IP SLA Responder

Formatted: Keep with next

Figure 1: IP SLA Architechture

Formatted: Caption

The IP SLA 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 SLA Responder need not be enabled. For non-Cisco devices the IP SLA Responder cannot be configured and the IP SLAs can send operational packets only to services native to those devices.

Deleted: s

Deleted: ,

Deleted: ,

Deleted: s

Deleted: ,

Deleted: s

Response Time Computation for Cisco IOS 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 in a queue while waiting to be processed. In this situation the response times would not accurately represent true network delays. Cisco IOS IP SLA minimizes 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 allow accurate true round-trip times to be calculated. IP SLA test packets use time stamping to minimize the effect of processing delays.

Deleted: ,

Deleted: o

Deleted: ,

Deleted: s

Deleted: ,

Deleted: determine

Deleted: s

When enabled the IP SLA 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

Deleted: ,

Deleted: s

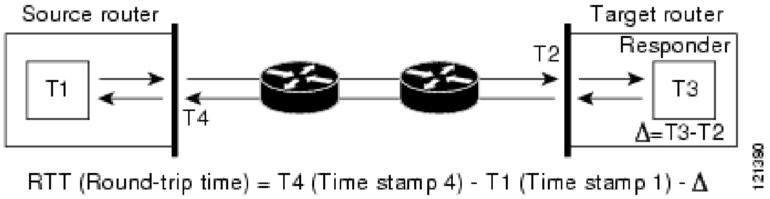
Deleted: ,

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 2 below 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.

Deleted: The f

Deleted: ,


Source router
Target router
T2
Responder
T1
T3
T4
Δ=T3-T2
RTT (Round-trip time) = T4 (Time stamp 4) - T1 (Time stamp 1) - Δ
121380

Formatted: Keep with next

Figure 2: Time Stamping Packets to Eliminate Packet Processing Delay

Formatted: Caption

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 behaviour 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.

Deleted: behavior

Deleted: ,

Cisco IOS IP SLAs Operation Scheduling

Formatted: Font: (Default) Arial, (Asian) Times New Roman, 14 pt, Bold, Italic, Complex Script Font: Arial Unicode MS, 14 pt, (Complex) , English U.S.

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 can be delayed to start on 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.

Deleted: start at a

Multiple operation 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 SLA 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 SLA operations should start. This feature automatically distributes the IP SLA operations at equal intervals over a

Deleted: s

Deleted: s

Deleted: s

Deleted: s

Deleted: s

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 ip sla 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.

The IP SLAs multiple operation 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 SLA displays a message showing the number of active and missing operations.

Deleted: s

Deleted: s

A main benefit for scheduling multiple IP SLA 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.

Deleted: s

Deleted: ,

Deleted: ,

Operations of the same type and same frequency should be used for IP SLAs multiple operation 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.

Deleted: s

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

Cisco IOS IP SLAs Operation Thresholds

To support successful service level agreement monitoring or to proactively measure network performance, threshold functionality becomes essential. Consistent reliable measurements immediately identify issues and can save troubleshooting time. To confidently roll out a service level agreement you need to have mechanisms that notify you immediately of any possible violation. IP SLAs can send SNMP traps triggered by the following events:

- Connection loss
- Timeout
- Round-trip time threshold
- Average jitter threshold
- One-way packet loss
- One-way jitter
- One-way mean opinion score (MOS)
- One-way latency

Alternately, an IP SLAs threshold violation can trigger another IP SLAs operation for further analysis. For example, the frequency could be increased or an ICMP Path Echo or ICMP Path Jitter operation could be initiated for troubleshooting.

Determining the type of threshold and the level to set can be complex and it depends on the type of IP service being used in the network. For more details on using thresholds with IP SLAs operations, see the "IP SLAs—Proactive Threshold Monitoring" module.

Deleted: ,

Playing Around

With this lab, we would like you to experience IP SLAs. This is not a “copy and paste” lab – that would be too easy – so try to do the exercises yourself rather than looking at the solution. See Appendix A for how to access the network.

Deleted: ”

The lab is divided into sections and the instructor will brief you shortly after each of them. After the completion of this lab you will know how to configure and schedule a significant number of operations, to set your own policy (thresholds) and how to react policy violations. At the end of the lab, a more significant exercise will leverage all the features you have learned.

Deleted: ,

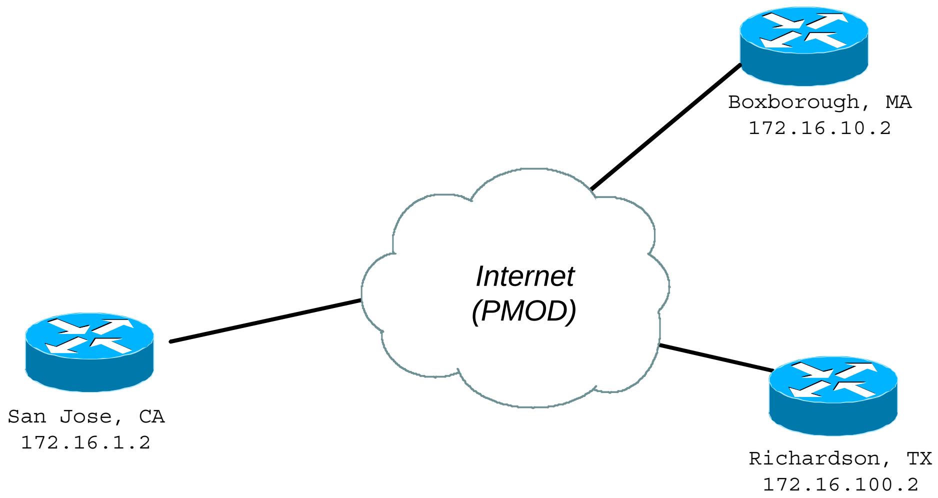
Deleted: ,

Deleted: large amount

Deleted: upon

Deleted: together

Lab Topology



UDP Jitter operation

Each operation consists of a set of different parameters. Operations are typically configured in two phases: configuration and scheduling. Each operation is identified through a single numeric identifier: this is a locally significant number, an index number.

For example, here is an example in which a UDP jitter operation has been configured on 172.16.1.2 (San Jose) to 172.16.10.2 (Boxborough), with destination port number 1234, and operation ID of 1:

Deleted: instance

Deleted: a sample to configure

Deleted: an

i)

```
ip sla 1
 udp-jitter 172.16.10.2 1234
```

Now, the operation has been configured. Check the status with this command:

ii)

```
SanJose#sh ip sla statistics 1 details

Round Trip Time (RTT) for       Index 1
Number of successes: Unknown
Number of failures: Unknown
Operation time to live: 0
Operational state of entry: Inactive
Last time this entry was reset: Never
```

The operation status is *inactive*. This means it has been configured, but it is not running. To start an operation, you can either schedule it directly, or a condition can trigger it. We will see the later below.

Let's schedule the operation to start now by configuring:

iii)

```
ip sla schedule 1 start-time now
```

Now you can try again and check the operation status:

iv)

```
SanJose#sh ip sla statistics 1 details

Round Trip Time (RTT) for       Index 1
        Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: *15:21:20.775 PST Wed Nov 2 2005
Latest operation return code: No connection
Over thresholds occurred: FALSE
RTT Values:
…
```

The status is "No Connection" because the target router does not respond to our request. Why is that? Just because we completely forgot to turn on the IP SLAs Responder! So let's configure it on Boxborough:

v)

```
Box(config)#ip sla responder
Box(config)#exit
Box#
*Nov  2 17:06:04.839: %SYS-5-CONFIG_I: Configured from console by
console
Box#sh ip sla responder
IP SLAs Responder is: Enabled
Number of control message received: 1 Number of errors: 0
Recent sources:
        172.16.1.2 [17:05:49.559 PST Wed Nov 2 2005]
Recent error sources:
```

Now that the responder is enabled, check again if the operation is working fine:

vi)

```
SanJose#sh ip sla stat 1

Round Trip Time (RTT) for       Index 1
        Latest RTT: 1 milliseconds
Latest operation start time: *17:09:40.087 PST Wed Nov 2 2005
Latest operation return code: OK
RTT Values:
        Number Of RTT: 10               RTT Min/Avg/Max: 1/1/4 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 0
        Source to Destination Latency one way Min/Avg/Max: 0/0/0
milliseconds
        Destination to Source Latency one way Min/Avg/Max: 0/0/0
milliseconds
Jitter Time:
        Number of Jitter Samples: 9
        Source to Destination Jitter Min/Avg/Max: 3/3/3 milliseconds
        Destination to Source Jitter Min/Avg/Max: 1/1/4 milliseconds
Packet Loss Values:
        Loss Source to Destination: 0           Loss Destination to Source: 0
        Out Of Sequence: 0      Tail Drop: 0    Packet Late Arrival: 0
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 0
        Mean Opinion Score (MOS): 0
Number of successes: 5
Number of failures: 0
Operation time to live: 3308 sec
```

Note the operation is now having a status of "OK". How many packets made the round trip time with success? Look at the different metrics, what is the minimum, average and maximum round trip time?

Deleted: did

Now, using the same technique, configure operations between the three routers for complete coverage of measurement. That is going to be three operations in total, since they are bidirectional.

UDP Jitter operation for VoIP applications

We have an IP performance metric for production traffic, this is good but it is not enough. Now, we would like to know how our voice class is performing. We will assume that voice carried over G711-alaw codec, port number is 16384 and the voice class has been configured with TOS of 48. For this, we will use the UDP Operation for VoIP.

Deleted: this

Deleted: our voice class

Deleted: ?

Therefore the configuration is almost the same as for the UDP Jitter operation, except that we need to: specify a Codec type and TOS value.

Here is a sample configuration from Boxborough to San Jose:

vii)

```
ip sla 3
 udp-jitter 172.16.1.2 16384 codec g711alaw
 tos 48
ip sla schedule 3 start-time now
```

Check the results with the same command as before. Pay a particular attention to MOS and ICPIF scores:

viii)

```
Box#sh ip sla stat 3

Round Trip Time (RTT) for       Index 3
        Latest RTT: 1111 microseconds
Latest operation start time: *18:03:08.391 PST Wed Nov 2 2005
Latest operation return code: OK
RTT Values:
        Number Of RTT: 839              RTT Min/Avg/Max: 1/1111/12000 microseconds
Latency one-way time:
        Number of Latency one-way Samples: 0
        Source to Destination Latency one way Min/Avg/Max: 0/0/0 microseconds
        Destination to Source Latency one way Min/Avg/Max: 0/0/0 microseconds
Jitter Time:
        Number of Jitter Samples: 838
        Source to Destination Jitter Min/Avg/Max: 1/4034/12000 microseconds
        Destination to Source Jitter Min/Avg/Max: 1/3193/8001 microseconds
Packet Loss Values:
        Loss Source to Destination: 0           Loss Destination to Source: 0
        Out Of Sequence: 0      Tail Drop: 0    Packet Late Arrival: 0
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 58
        Mean Opinion Score (MOS): 2.12
Number of successes: 5
Number of failures: 1
Operation time to live: 3252 sec
```

For further information, proceed to the "IP SLAs—Analyzing Service Levels Using the VoIP UDP Jitter Operation" documentation module.

IP SLAs Multiple Operation Scheduling

Deleted: *m*
Deleted: *o*
Deleted: *s*
Deleted: *s*

With IP SLAs running on a large network with multiple classes there are situations where the operation overhead begins to be quite significant. Assuming all the operations are scheduled with the option start-time now, we expose the router to a potential denial of service upon reload. Indeed, all the operations will start at the same time.

Deleted: ,
Deleted: amount of
Deleted: s
Deleted: large

This is bad for network metrics (not a realistic scenario), but also for the router’s resources. To elegantly workaround this problem the multi-operation scheduler has been invented. The IP SLAs Multiple Operation Scheduling feature provides the capability to easily schedule multiple IP SLA operations to begin at intervals equally distributed over a specified duration of time and to restart at a specified frequency. This special scheduler lets you bundle operations in a single group and schedule all of them smoothly over a period of time.

Deleted: elegantly
Deleted: ,
Deleted: d
Deleted: s
Deleted: ,

For example, configure 10 operations with indexes ranging from 10 to 19. Then schedule all the operations as group 1 at once over a period of 20 seconds, use this command:

Deleted: ,

ix)

```
ip sla group schedule 1 10-19 schedule-period 20 start-time now
```

But there is still one problem that may arise: all the operations are run in a very regular and sequential pattern. What if our test is actually running concurrently with something else, like a routing protocol update?

Deleted: Using the command of your choice, if the operations have been started within the appropriate time window.

That’s exactly why the possibility to “randomize” the start time has been provided. Stop the previous scheduling (by removing the group scheduling line) and now randomize the start-time of 5 seconds. The config would then be:

Deleted: Try to s

x)

```
ip    sla    group    schedule    1    10-19    schedule-period    20    \
    frequency range 55-65 start-time now
```

Every time the operation has run, the next start-time will be between 55 and 65 seconds later. This time is randomized over that range, and will change for each execution. Check with the appropriate command that the operations are randomized.

Deleted: if

Using thresholds with IP SLAs operations

IP SLAs can be configured to react to certain measured network conditions. For example, if IP SLA measures too much jitter on a connection then it can generate a notification to a network management application or trigger another IP SLA operation to gather more data.

Deleted: s

Deleted: , IP SLAs

Deleted: ,

Deleted: s

IP SLAs reaction configuration is performed using the **`ip sla reaction-configuration`** command. You can configure **`the ip sla reaction-configuration`** command multiple times so as to allow reactions for multiple monitored elements (for example, configuring thresholds for operation 1 for destination-to-source packet loss, and also configuring MOS thresholds for same operation). You can check the configuration of the IP SLAs reaction configuration using the show ip sla reaction-configuration command.

In order to test the mechanism, configure on San Jose a jitter operation with index number 1 and with the following characteristics:

- Send 1000 packets
- Interval on 20 ms
- Frequency of 30 seconds
- Immediate scheduling with infinite life

Then we would like to immediately send an SNMP trap to the network management station 1.1.1.1, with the community string 'ipsla' if our round trip time delay for this operation is over 20 ms two times out of three. If the RTT drop below 10ms then we can clear the alert.

Deleted: ,

Deleted: immediately

Deleted:

First we need to enable the trap sending to the server and we will also enable debugs so that we can see traps leaving the router:

Deleted: ,

xi)

```
SanJose(config)#snmp-server enable traps rtr
SanJose(config)#snmp-server host 1.1.1.1 ipsla
SanJose(config)#end
*Nov  3 20:04:03.669: %SYS-5-CONFIG_I: Configured from
console by console
SanJose#debug snmp packets
SNMP packet debugging is on
```

Then, we need to configure a reaction config for operation 1, like this:

xii)

```
ip sla reaction-configuration 1 react rtt threshold-value
20 10 threshold-type xOfy 2 3 action-type trapOnly
```

Now check the operation status, we are under threshold so everything is all right. In order to force the delay up, we will shape down the traffic on San Jose outgoing interface. Configure this:

Deleted: to go

xiii)

```
SanJose(config)#int e0/0
SanJose(config-if)#traffic-shape rate 12000
SanJose(config-if)#end
```

This should increase significantly the delay, and therefore you should be able to see the SNMP trap fired out (be sure the debugs are enabled):

xiv)

```
SanJose#
*Nov  3 19:57:03.505: SNMP: Queuing packet to 1.1.1.1
*Nov  3 19:57:03.505: SNMP: V1 Trap, ent rttMonNotificationsPrefix,
addr 172.16.1.2, gentrap 6, spectrap 5
 rttMonCtrlAdminTag.1 =
 rttMonHistoryCollectionAddress.1 = AC 10  0A 02
 rttMonCtrl.19.1.2.1 = 1
 rttMonCtrl.19.1.10.1 = 1
 rttMonCtrl.19.1.9.1 = 1
 rttMonCtrl.19.1.5.1 = 20
 rttMonCtrl.19.1.6.1 = 10
 rttMonEchoAdminEntry.33.1 = 00 00  00 00
*Nov  3 19:57:03.773: SNMP: Packet sent via UDP to 1.1.1.1
```

Now, try to remove the shaping on the interface. Once the delay is below 10 ms, check if the trap is cleared.

Deleted: will go

xv)

```
*Nov  3 21:07:33.512: SNMP: Queuing packet to 1.1.1.1
*Nov  3 21:07:33.512: SNMP: V1 Trap, ent rttMonNotificationsPrefix,
addr 172.16.1.2, gentrap 6, spectrap 5
 rttMonCtrlAdminTag.1 =
 rttMonHistoryCollectionAddress.1 = AC 10  0A 02
 rttMonCtrl.19.1.2.1 = 1
 rttMonCtrl.19.1.10.1 = 2
 rttMonCtrl.19.1.9.1 = 312
 rttMonCtrl.19.1.5.1 = 20
 rttMonCtrl.19.1.6.1 = 10
 rttMonEchoAdminEntry.33.1 = 00 00  00 00
*Nov  3 21:07:33.780: SNMP: Packet sent via UDP to 1.1.1.1
```

Go a little further

Now, you will reuse what we have seen and a little bit more to configure the following scenario. Feel free to use IP SLA documentation to help you.

Deleted: s'

From all routers to all routers, configure one VoIP operation with the codec of your choice. If that operation fails (not over threshold, but a failure) then fallback to an ICMP ping operation and send a trap. Indeed, it might be that the responder on the other side has been turned off, so the reachability is still there but the jitter operation fails. If both the jitter and ping operations fail too, then send another trap.

Deleted: s

Try to disable the responder at one place, and see if the other routers are falling back into ICMP echo mode. Then try to kill connectivity. You can shutdown the destination interface to disable connectivity completely and then verify if the traps are sent.

Deleted: the connectivity,

Documentation

If needed, you can also access IP SLAs home page containing some marketing material here:

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