Implementing IP Service Level Agreements

IP Service Level Agreements (IP SLAs) is a portfolio of technologies embedded in most devices that run Cisco IOS XR Software, which allows the user to perform network assessments, verify quality of service (QoS), ease the deployment of new services, and assist administrators with network troubleshooting and so on.

This chapter provides information about this feature and the different steps involved in configuring it.

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.3.1</td>
<td>Two-Way Active Measurement Protocol (TWAMP) was introduced.</td>
</tr>
</tbody>
</table>

This chapter covers the following topics:

- IP Service Level Agreements Technology Overview, on page 1
- Prerequisites for Implementing IP Service Level Agreements, on page 3
- Restrictions for Implementing IP Service Level Agreements, on page 3
- Measuring Network Performance with IP Service Level Agreements, on page 4
- Two-Way Active Measurement Protocol (TWAMP), on page 6

**IP Service Level Agreements Technology Overview**

IP SLA uses active traffic monitoring, which generates traffic in a continuous, reliable, and predictable manner to measure network performance. IP SLA sends data across the network to measure performance between multiple network locations or across multiple network paths. It simulates network data and IP services, and collects network performance information in real time. The following information is collected:

- Response times
- One-way latency, jitter (inter-packet delay variance)
- Packet loss
- Network resource availability

IP SLA performs active monitoring by generating and analyzing traffic to measure performance, either between the router or from a router to a remote IP device such as a network application server. Measurement statistics,
which are provided by the various IP SLA operations, are used for troubleshooting, problem analysis, and designing network topologies.

This section covers the following topics:

Service Level Agreements

Internet commerce has grown significantly in the past few years as the technology has advanced to provide faster, more reliable access to the Internet. Many companies need online access and conduct most of their business online and conduct most of their business on line and any loss of service can affect the profitability of the company. Internet service providers (ISPs) and even internal IT departments now offer a defined level of service—a service level agreement—to provide their customers with a degree of predictability.

Network administrators are required to support service level agreements that support application solutions. Figure 1: Scope of Traditional Service Level Agreement Versus IP SLA, on page 2 shows how IP SLA has taken the traditional concept of Layer 2 service level agreements and applied a broader scope to support end-to-end performance measurement, including support of applications.

This table lists the improvements with IP SLA over a traditional service level agreement.

Table 2: IP SLA Improvements over a Traditional Service Level Agreement

<table>
<thead>
<tr>
<th>Type of Improvement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-to-end measurements</td>
<td>The ability to measure performance from one end of the network to the other allows a broader reach and more accurate representation of the end-user experience.</td>
</tr>
<tr>
<td>Sophistication</td>
<td>Statistics, such as delay, jitter, packet sequence, Layer 3 connectivity, and path and download time, that are divided into bidirectional and round-trip numbers provide more data than just the bandwidth of a Layer 2 link.</td>
</tr>
<tr>
<td>Accuracy</td>
<td>Applications that are sensitive to slight changes in network performance require the precision of the submillisecond measurement of IP SLA.</td>
</tr>
<tr>
<td>Ease of deployment</td>
<td>Leveraging the existing Cisco devices in a large network makes IP SLA easier to implement than the physical operations that are often required with traditional service level agreements.</td>
</tr>
<tr>
<td>Application-aware monitoring</td>
<td>IP SLA can simulate and measure performance statistics generated by applications running over Layer 3 through Layer 7. Traditional service level agreements can measure only Layer 2 performance.</td>
</tr>
</tbody>
</table>
IP SLA support exists in Cisco networking devices ranging from low-end to high-end routers and switches. This wide range of deployment gives IP SLA more flexibility over traditional service level agreements.

### Benefits of IP Service Level Agreements

This table lists the benefits of implementing IP SLA.

**Table 3: List of Benefits for IP SLA**

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP SLA monitoring</td>
<td>Provides service level agreement monitoring, measurement, and verification.</td>
</tr>
<tr>
<td>Network performance monitoring</td>
<td>Measure the jitter, latency, or packet loss in the network. In addition, IP SLA provides continuous, reliable, and predictable measurements along with proactive notification.</td>
</tr>
<tr>
<td>IP service network health assessment</td>
<td>Verifies that the existing QoS is sufficient for the new IP services.</td>
</tr>
<tr>
<td>Troubleshooting of network operation</td>
<td>Provides consistent, reliable measurement that immediately identifies problems and saves troubleshooting time.</td>
</tr>
</tbody>
</table>

### Prerequisites for Implementing IP Service Level Agreements

Knowledge of general networking protocols and your specific network design is assumed. Familiarity with network management applications is helpful. We do not recommend scheduling all the operations at the same time as this could negatively affect your performance.

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

### Restrictions for Implementing IP Service Level Agreements

- The maximum number of IP SLA operations that is supported by Cisco IOS XR Software is 2048.
- The maximum number of IP SLA configurable operations that is supported by Cisco IOS XR Software is 2000.
- We do not recommend scheduling all the operations at the same start time as this may affect the performance. At the same start time, not more than 10 operations per second should be scheduled. We recommend using the `start after` configuration.
Setting the frequency to less than 60 seconds will increase the number of packets sent. But this could negatively impact the performance of IP SLA operation when scheduled operations have same start time.

- IP SLA is not HA capable.
- Consider the following guidelines before configuring the frequency, timeout, and threshold commands.

## Measuring Network Performance with IP Service Level Agreements

IP SLA uses generated traffic to measure network performance between two networking devices, such as routers. Figure 2: IP SLA Operations, on page 4 shows how IP SLA starts when the IP SLA device sends a generated packet to the destination device. After the destination device receives the packet and if the operation uses an IP SLA component at the receiving end (for example, IP SLA Responder), the reply packet includes information about the delay at the target device. The source device uses this information to improve the accuracy of the measurements. An IP SLA operation is a network measurement to a destination in the network from the source device using a specific protocol, such as User Datagram Protocol (UDP) for the operation.

**Figure 2: IP SLA Operations**

To implement IP SLA network performance measurement, perform these tasks:

1. Enable the IP SLA Responder, if appropriate.
2. Configure the required IP SLA operation type.
3. Configure any options available for the specified IP SLA operation type.
4. Configure reaction conditions, if required.
5. Schedule the operation to run. Then, let the operation run for a period of time to gather statistics.
6. Display and interpret the results of the operation using Cisco IOS-XR Software CLI, XML, or an NMS system with SNMP.

The following topics are covered in this section:
IP SLA Responder and IP SLA Control Protocol

The IP SLA Responder is a component embedded in the destination Cisco routing device that allows the system to anticipate and respond to IP SLA request packets. The IP SLA Responder provides enhanced accuracy for measurements. The patented IP SLA Control Protocol is used by the IP SLA Responder, providing a mechanism through which the responder is notified on which port it should listen and respond. Only a Cisco IOS-XR software device or other Cisco platforms can be a source for a destination IP SLA Responder.

Figure 2: IP SLA Operations, on page 4 shows where the IP SLA Responder fits relative to the IP network. The IP SLA Responder listens on a specific port for control protocol messages sent by an IP SLA operation. Upon receipt of the control message, the responder enables the UDP port specified in the control message 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 SLA packet or packets, or when the specified time expires. For added security, MD5 authentication for control messages is available.

Note

The IP SLA responder needs at least one second to open a socket and program Local Packet Transport Services (LPTS). Therefore, configure the IP SLA timeout to at least 2000 milli seconds.

The IP SLA Responder must be used with the UDP jitter operation. If services that are already provided by the target router are chosen, the IP SLA Responder need not be enabled. For devices that are not Cisco devices, the IP SLA Responder cannot be configured, and the IP SLA can send operational packets only to services native to those devices.

Response Time Computation for IP SLA

Because of other high-priority processes, routers can take tens of milliseconds to process incoming packets. The 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. IP SLA minimizes these processing delays on the source router and on the target router (if IP SLA Responder is being used) to determine true round-trip times. Some IP SLA probe packets contain delay information that are used in the final computation to make measurements more accurate.

When enabled, the IP SLA Responder allows the target device to take two time stamps, both when the packet arrives on the interface and again just as it is leaving, and accounts for it when calculating the statistics. This time stamping is made with a granularity of submilliseconds.

Figure 3: IP SLA Responder Time Stamping, on page 6 shows how the responder works. T3 is the time the reply packet is sent at the IP SLA Responder node, and T1 is the time the request is sent at the source node. 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 SLA on the source router on which the incoming time stamp 4 (TS4) is taken in a high-priority path to allow for greater accuracy.
**IP SLA Operation Scheduling**

After an IP SLA operation is configured, you must schedule the operation to begin capturing statistics and collecting error information. When scheduling an operation, the operation starts immediately or starts at a certain month and day. In addition, an operation can be scheduled to be in pending state, which is used when the operation is a reaction (threshold) operation waiting to be triggered. Normal scheduling of IP SLA operations lets you schedule one operation at a time.

**Two-Way Active Measurement Protocol (TWAMP)**


**Advantages of TWAMP**

- TWAMP enables complete IP performance measurement.
- TWAMP provides a flexible choice of solutions as it supports all devices deployed in the network.

The following topics are the covered in this section:

**The TWAMP Entities**

The TWAMP system consists of 4 logical entities:

- server - manages one or more TWAMP sessions and also configures per-session ports in the end-points.
- session-reflector - reflects a measurement packet as soon as it receives a TWAMP test packet.
- control-client - initiates the start and stop of TWAMP test sessions.
- session-sender - instantiates the TWAMP test packets sent to the session reflector.

The below diagram shows TWAMP implementation where TWAMP runs on two separate hosts. One plays the roles of Control-Client and Session-Sender, and the other plays the roles of Server and Session-Reflector. Cisco NCS 5500 Series router supports Session-Server and Session Reflector functionality only. Using TWAMP, the IP performance of underlying transport can be measured through cooperation between network elements that include TWAMP support.
The TWAMP protocol includes three distinct message exchange categories, they are:

- **Connection set-up exchange**: Messages establish a session connection between the Control-Client and the Server. First the identities of the communicating peers are established via a challenge response mechanism. The Server sends a randomly generated challenge, to which the Control-Client then sends a response by encrypting the challenge using a key derived from the shared secret. Once the identities are established, the next step negotiates a security mode that is binding for the subsequent TWAMP-Control commands as well as the TWAMP-Test stream packets.

  ![Figure 4: The TWAMP Entities](image)

- **TWAMP-control exchange**: The TWAMP-Control protocol runs over TCP and is used to instantiate and control measurement sessions. Unlike the Connection setup exchanges, the TWAMP-Control commands can be sent multiple times. However, the messages cannot occur out of sequence although multiple request-session commands can be sent before a session-start command. The sequence of commands is as follows:
  - request-session
  - start-session
  - stop-session

- **TWAMP-test stream exchange**: The TWAMP-Test runs over UDP and exchanges TWAMP-Test packets between Session-Sender and Session-Reflector. These packets include timestamp fields that contain the instant of packet egress and ingress. In addition, each packet includes an error-estimate that indicates the synchronization skew of the sender (session-sender or session-reflector) with an external time source (e.g. GPS or NTP). The packet also includes a Sequence Number.

TWAMP-Control and TWAMP-test stream, have three security modes: unauthenticated, authenticated, and encrypted.
Restrictions of TWAMP on the NCS 5500 Series Router

- Cisco NCS 5500 Series router supports only Session-Server and Session Reflector functionality.
- Hardware Timestamp feature which provides greater accuracy is not supported.

Configuring TWAMP on the NCS 5500 Series Router

Configuration of Session-Server

Router# configure
Router(config)# ipsla server twamp
Router(config-ipsla-server-twamp)# port 862
Router(config-ipsla-server-twamp)# commit

Configuration of Session-Reflector

Router# configure
Router(config)# ipsla responder twamp
Router(config-twamp-ref)# commit

Running Configuration

ipsla
responder
twamp
!
server twamp
port 862
!
!

Verification of TWAMP feature on the NCS 5500 Series Router

The status of the TWAMP feature can be verified using the command `show ipsla twamp status`

Router# show ipsla twamp status
Thu Aug 17 12:42:38.923 IST
TWAMP Server is enabled
TWAMP Server port : 862
TWAMP Reflector is enabled

The TWAMP session can be verified using the command `show ipsla twamp session`

Router# show ipsla twamp session
IP SLAs Responder TWAMP is: Enabled
Recvr Addr: 10.5.139.11
Recvr Port: 7222
Sender Addr: 172.27.111.233
Sender Port: 33243
Session Id: 10.5.139.11:70929508:88F7A620
Connection Id: 0

The TWAMP test session based on source ip-address can be verified using the command `show ipsla twamp session source-ip <source ip-address> source-port <source port-number>`
RP/0/0/CPU0:ios# show ipsla twamp session source-ip 172.27.111.233 source-port 33286
IP SLAs Responder TWAMP is: Enabled
Recvr Addr: 10.5.139.11
Recvr Port: 6198
Sender Addr: 172.27.111.233
Sender Port: 33286
Session Id: 10.5.139.11:71804476:F2721505
Connection Id: D
Mode: Unauthorized
DSCP: 0
Pad Length: 0
Number of Packets Received: 8867
Verification of TWAMP feature on the NCS 5500 Series Router