



## What is Cisco IP SLA?

---

Cisco IP Service Level Agreement (IP SLA) is software built into Cisco IOS for monitoring application response times with synthetic packets between two network end-points. IP SLA data can be harvested with a SNMP monitoring solution by retrieving the data directly from the router or switch's IOS. But why should you deploy Cisco IP SLA?

Application response times are at the heart of application delivery management. The speed of the application's responses to the end user's requests will ultimately determine whether the user's experience using that application is excellent, adequate, or unacceptable. While measuring real application transactions is the most accurate method for measuring response times, sometimes that approach is not an option. For example, during the pre-deployment assessment phase of rolling out a new application, or when measuring a service provider SLA edge-to-edge, real transactions that would be applicable to the usage scenarios you need to test are not being performed. It's in such situations where synthetic transactions, generated and measured by the Cisco IP SLA functionality, can offer some assistance.

IP SLA is built into almost every model of Cisco router and switch, from the access-layer devices to the core, including the Catalyst 6500 and 7600 Series. Because it is included in the Cisco equipment, IP SLA does not require additional licenses or hardware to operate. The IP SLA capabilities can simply be activated through the device's command line interface (CLI) or through an SNMP polling product with the appropriate credentials. Once IP SLA is enabled, the configuration and reporting can begin immediately.

IP SLA operates by sending synthetic transactions between two network devices or between a network device and a server. One device acts as the "sender" of the test data, and the other acts as the "responder." The sender can be configured to send different types of synthetic transactions based on port, packet size, type of service, and even more advanced characteristics, as is the case with Voice over Internet Protocol (VoIP) tests. Table 1 below lists some of the different IP SLA test types.

Test Name	Measurement Capability	Example Use
UDP Jitter	UDP Jitter Round-trip delay, one-way delay, one-way jitter, one-way packet loss. One-way delay requires time synchronization between the Cisco IOS IP SLAs source and target routers	Validating and monitoring delay for latency-sensitive UDP applications
UDP Echo	Round-trip delay	Validating and monitoring delay for specific UDP applications
UDP Jitter for VoIP	Round-trip delay, one-way delay, one-way jitter, one-way packet loss, VoIP codec simulation: G.711 ulaw, G.711 alaw, and G.729a MOS, and ICPIF voice quality scoring capability. One-way delay requires time synchronization between the Cisco IOS IP SLA source and target routers.	Validating and monitoring VoIP environments, especially prior to rolling out VoIP or investing in VoIP infrastructure
TCP Connect	Connection time	Validating and monitoring delay for connection establishment on TCP applications
Domain Name System (DNS)	DNS lookup time	Validating and monitoring DNS resolution times across the network
Dynamic Host Configuration Protocol (DHCP)	Round-trip time to get an IP address	Validating and monitoring DHCP lookup times across the network

FTP	Round-trip time to transfer a file	Validating and monitoring file transfer times using the FTP protocol across the network
HTTP	Round-trip time to get a Web page	Validating and monitoring Web transactions across the network
Internet Control Message Protocol (ICMP) Echo	Round-trip delay	Validating and monitoring delay for ping response times over the ICMP protocol
ICMP Path Echo	Round-trip delay for the full path	Validating and monitoring service provider latency SLAs at all levels of service
ICMP Path Jitter	Round-trip delay, jitter, and packet loss for the full path	Validating and monitoring service provider latency and delivery SLAs at all levels of service

Once the sender is configured with the desired IP SLA test parameters, packets are sent to the selected responder. Emulating a typical client-server interaction, the responder sends a response packet back to the sender. The sender then calculates the response-time metrics appropriate for the test type, and the process repeats multiple times, based on the test configuration.

Extracting the IP SLA response-time metrics directly from routers and switches can be difficult, but tools are available with monitoring capabilities that can greatly ease this situation. Instead of relying on the device CLI for copying metrics from a Telnet session to a spreadsheet for graphing purposes, you can deploy an SNMP polling product to collect data automatically, directly from the device. Given the proper credentials, this class of product can extract the response-time metrics recorded during IP SLA testing, store them in a database, and display the results in a graphical user interface. Some SNMP polling products can also provide analytical function beyond data

collection, such as calculating baselines, displaying trends, and triggering threshold alerts based on collected IP SLA data. Cisco IP SLA should be part of every network manager's toolbox for managing application delivery. As a free component of Cisco routers and switches, it provides numerous benefits once you've enabled it and have begun running it as part of any new application pre-deployment program.

An SNMP polling product with application-aware monitoring capabilities is similarly essential to an application-aware approach to the network. While IP SLA is an extremely powerful data source, collecting metrics from a CLI can be time-consuming, and raw data has only limited usefulness for most IT staff.