



IP SLAs—Proactive Threshold Monitoring of IP SLAs Operations

First Published: August 14, 2006
Last Updated: July 16, 2008

This document describes the proactive monitoring capabilities of Cisco IOS IP Service Level Agreements (SLAs) using thresholds and reaction triggering.

Cisco IOS IP SLAs allows you to monitor, analyze and verify IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce occurrences of network congestion or outages. IP SLAs uses active traffic monitoring for measuring network performance.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for IP SLAs Proactive Threshold Monitoring](#)” section on page 11.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Information About Proactive Threshold Monitoring for IP SLAs](#), page 2
- [How to Configure IP SLAs Reactions and Threshold Monitoring](#), page 3
- [Configuration Examples for Proactive Threshold Monitoring Using IP SLA](#), page 6
- [Where to Go Next](#), page 9
- [Additional References](#), page 9
- [Feature Information for IP SLAs Proactive Threshold Monitoring](#), page 11



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2006 Cisco Systems, Inc. All rights reserved.

Information About Proactive Threshold Monitoring for IP SLAs

To perform the tasks required to configure proactive threshold monitoring using IP SLA, you should understand the following concepts:

- [IP SLAs Reaction Configuration, page 2](#)
- [IP SLAs Threshold Monitoring and Notifications, page 2](#)

IP SLAs Reaction Configuration

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

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). However, issuing the **no ip sla reaction-configuration operation-number** will clear all reactions for the specified operation. In other words, disabling of granular reaction elements (**no ip sla reaction-configuration operation-number react monitored-element**) is not currently supported, so as to provide backwards compatibility with the earlier version of this command.

You can check the configuration of the IP SLAs reaction configuration using the **show ip sla reaction-configuration** command.

IP SLAs Threshold Monitoring and Notifications

IP SLAs includes the capability for triggering SNMP notifications based on defined thresholds. This allows for proactive monitoring in an environment where IT departments can be alerted to potential network problems, rather than having to manually examine data.

IP SLAs supports threshold monitoring for performance parameters such as average jitter, unidirectional latency and bidirectional round trip time and connectivity. This proactive monitoring capability provides options for configuring reaction thresholds for important VoIP related parameters including unidirectional jitter, unidirectional packet loss, and unidirectional VoIP voice quality scoring (MOS scores).

IP SLAs can generate system logging (syslog) messages when a reaction condition occurs. These system logging messages can then be sent as SNMP notifications (traps) using the CISCO-RTTMON-MIB.

For packet loss and jitter, notifications can be generated for violations in either direction (source to destination and destination to source) or for round trip values. Packet loss, jitter and MOS statistics are specific to IP SLAs Jitter operations. Notifications can also be triggered for other events, such as round-trip-time violations, for most IP SLAs monitoring operations.

SNMP notifications (traps) for IP SLAs can be configured as a triggered action, to be sent when monitored values exceed an upper threshold or fall below a lower threshold, or when a set of defined conditions are met. For example, an SNMP trap can be triggered by 5 consecutive timeouts during an IP SLAs operation. The sending of SNMP traps is one of the options for triggered actions that can be configured for IP SLAs violations. The monitored values (also called monitored elements), the threshold type, and the triggered action are configured using the **ip sla reaction-configuration** global configuration mode command.

SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB and CISCO-SYSLOG-MIB. Use the **ip sla logging traps** command to enable the generation of SNMP system logging messages specific to IP SLAs trap notifications. Use the **snmp-server enable traps rtr** command to enable the sending of IP SLAs SNMP trap notifications.

**Note**

Severity levels in the CISCO-SYSLOG-MIB are defined as follows:

```
SyslogSeverity INTEGER { emergency(1), alert(2), critical(3), error(4), warning(5), notice(6), info(7), debug(8) }
```

The values for severity levels are defined differently for the system logging process in Cisco IOS software: { emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debugging (7) }.

This means that IP SLAs Threshold violations are logged as level 6 (informational) within the logging process, but are sent as level 7 (info) traps from the CISCO-SYSLOG-MIB.

How to Configure IP SLAs Reactions and Threshold Monitoring

IP SLAs Reactions are configured using the **ip sla reaction-configuration** command. The elements of this command are described in the following sections

- [Configuring Monitored Elements for IP SLAs Reactions, page 3](#)
- [Configuring Threshold Violation Types for IP SLAs Reactions, page 5](#)
- [Specifying Reaction Events, page 6](#)

Configuring Monitored Elements for IP SLAs Reactions

IP SLAs reactions are configured to be triggered when a monitored value exceeds or falls below a specified level, or when a monitored event (such as a timeout or connection loss) occurs. These monitored values and events are called monitored elements. Descriptions of some of the types of monitored elements available are described in the following sections:

- [Configuring Triggers for Round-Trip-Time Violations, page 3](#)
- [Configuring Triggers for Jitter Violations, page 4](#)
- [Configuring Triggers for Packet Loss Violations, page 4](#)
- [Configuring Triggers for Mean Opinion Score Violations, page 5](#)

You can configure the **ip sla reaction-configuration** command multiple times so as to allow reactions for multiple monitored elements (for example, configuring a threshold for operation 1 for destination-to-source packet loss, and also configuring a MOS threshold for the same operation). However, entering the **no ip sla reaction-configuration operation-number** command will clear all reactions for the specified operation (in other words, disabling of granular reaction elements is not currently supported, so as to provide backwards compatibility with the earlier version of this command).

Configuring Triggers for Round-Trip-Time Violations

Round-trip-time (rtt) is one of the monitored values of all IP SLAs operations. Events (such as traps) can be triggered when the rtt value rises above a specified threshold, or when it falls below a specified threshold. To configure rtt as the monitored element, use the following version of the **ip sla reaction-configuration** command:

Command or Action	Purpose
<pre>ip sla reaction-configuration operation-number react rtt [threshold-type violation-condition] threshold-value upper-threshold lower-threshold [action-type {trapOnly triggerOnly trapAndTrigger}]</pre> <p>Example:</p> <pre>Router# ip sla reaction-configuration 10 react rtt threshold-type immediate threshold-value 5000 3000 action-type trapAndTrigger</pre>	Configures an action (SNMP trap or IP SLAs trigger) to occur based on violations of thresholds for round-trip-time (rtt).

Configuring Triggers for Jitter Violations

Jitter (interpacket delay variance) is one of the monitored values of IP SLAs UDP Jitter operations. Jitter values are computed as source-to-destination, destination-to-source, and combined round-trip values. Events (such as traps) can be triggered when the average jitter value in either direction, or in both directions, rises above a specified threshold, or when it falls below a specified threshold.

Command or Action	Purpose
<pre>ip sla reaction-configuration operation-number react {jitterAvg jitterDSAvg jitterSDAvg} [threshold-type violation-type] threshold-value upper-threshold lower-threshold [action-type {trapOnly triggerOnly trapAndTrigger}]</pre> <p>Example:</p> <pre>Router# ip sla reaction-configuration 10 react jitterAvg threshold-type immediate threshold-value 5000 3000 action-type trapAndTrigger</pre>	<p>Configures an action (SNMP trap or IP SLAs trigger) to occur based on violations of thresholds for average round-trip jitter values.</p> <ul style="list-style-type: none"> To configure the average source-to-destination jitter as the monitored element, use the react jitterAvg keyword combination. To configure average destination-to-source jitter as the monitored element, use the react jitterDSAvg keyword combination. To configure average round-trip jitter as the monitored element, use the react jitterSDAvg keyword combination.

Configuring Triggers for Packet Loss Violations

Packet loss is one of the monitored values of IP SLAs UDP Jitter operations. Jitter values are computed as source-to-destination and destination-to-source values. Events (such as traps) can be triggered when the jitter value in either direction rises above a specified threshold, or when it falls below a specified threshold.

To configure source-to-destination packet loss as the monitored element, use the **react PacketLossSD** syntax in the **ip sla reaction-configuration** command.

To configure destination-to-source jitter as the monitored element, use the **react PacketLossDS** syntax in the **ip sla reaction-configuration** command.

Configuring Triggers for Mean Opinion Score Violations

Mean opinion score (MOS) is one of the monitored values of IP SLAs Jitter VoIP operations. MOS values are computed as numbers to two decimal places, from a value of 1.00 (worst quality) to 5.00 (best quality). Events (such as traps) can be triggered when the MOS value in either direction rises above a specified threshold, or when it falls below a specified threshold.

To configure destination-to-source jitter as the monitored element, use the **react mos** syntax in the **ip sla reaction-configuration** command.

Configuring Threshold Violation Types for IP SLAs Reactions

The threshold-type syntax of the **ip sla reaction-configuration** command defines the type of threshold violation (or combination of threshold violations) that will trigger an event. Threshold violation types are as follows:

- **immediate**—Triggers an event immediately when the value for a reaction type (such as response time) exceeds the upper threshold value or falls below the lower threshold value, or when a timeout, connectionLoss, or verifyError event occurs.
- **consecutive**—Triggers an event only after a violation occurs a specified number of times consecutively. For example, the consecutive violation type could be used to configure an action to occur after a timeout occurs 5 times in a row, or when the round-trip-time exceeds the upper threshold value 5 times in a row.
- **x of y**—Triggers an event after some number (x) of violations within some other number (y) of probe operations (x of y).
- **averaged**—Triggers an event when the averaged totals of a value for x number of probe operations exceeds the specified upper-threshold value, or falls below the lower-threshold value.

Configuring these threshold violation types is described in the following sections.

Generating Events for Each Violation

To generate a trap (or trigger another operation) each time a specified condition is met, use the **immediate** threshold-type keyword:

```
ip sla reaction-configuration operation-number react data-type threshold-type immediate
threshold-value raising-value falling-value action-type action-value
```

Generating Events for Consecutive Violations

To generate a trap (or trigger another operation) after a certain number (x) of consecutive violations, use the consecutive keyword with the optional number-of-occurrences argument:

```
ip sla reaction-configuration operation-number react reaction-condition threshold-type consecutive
[number-of-occurrences] threshold-value raising-value falling-value action-type action-value
```

The default value for *number-of-occurrences* is 5.

Generating Events for x of y Violations

To generate a trap (or trigger another operation) after some number (x) of violations within some other number (y) of probe operations (x of y), use the **xofy** [*x-value y-value*] syntax:

ip sla reaction-configuration *operation-number* **react** *reaction-condition* **threshold-type** **xofy** *x-value* *y-value* **threshold-value** *raising-value* *falling-value* **action-type** *action-value*

The default x-value and y-value is 5 (**xofy 5 5**).

Generating Events for Averaged Violations

To generate a trap (or trigger another operation) when the averaged totals of x number of probe operations violate a falling-threshold or rising-threshold, use the **average** [*attempts*] syntax:

ip sla reaction-configuration *operation-number* **react** *reaction-condition* **threshold-type** **average** [*attempts*] **threshold-value** *raising-value* *falling-value* **action-type** *action-value*

The default value for *attempts* is 5.

Specifying Reaction Events

Action type options for the **ip sla reaction-configuration** command are as follows:

none—No action is taken.

trapOnly—Send an SNMP logging trap when the specified violation type occurs for the monitored element. IP SLAs logging traps are enabled using the **ip sla logging traps** command. For SNMP logging traps to be sent, SNMP logging must be enabled using the appropriate SNMP commands, including the **snmp-server enable traps syslog** command.

triggerOnly—Have one or more target operation's operational state make the transition from "pending" to "active" when the violation conditions are met. The target operations to be triggered are specified using the **ip sla reaction-trigger** command. A target operation will continue until its life expires, as specified by the target operation's configured lifetime value). A triggered target operation must finish its life before it can be triggered again.

trapAndTrigger—Trigger both an SNMP trap and start another IP SLAs operation when the violation conditions are met, as defined in the **trapOnly** and **triggerOnly** options above.

Configuration Examples for Proactive Threshold Monitoring Using IP SLA

This section contains the following configuration examples:

- [Configuring an IP SLAs Reaction Configuration: Example, page 6](#)
- [Verifying an IP SLAs Reaction Configuration: Example, page 7](#)
- [Triggering SNMP Notifications: Example, page 8](#)

Configuring an IP SLAs Reaction Configuration: Example

In the following example, IP SLAs operation 10 (a UDP Jitter operation) is configured to send an SNMP logging trap when the MOS value exceeds 4.9 (best quality) or falls below 2.5 (poor quality):

```
Router(config)# ip sla reaction-configuration 10 react mos threshold-type immediate
threshold-value 490 250 action-type trapOnly
```

The following example shows the default settings for the **ip sla reaction-configuration** command when none of the optional syntax is used:

```
Router# show ip sla reaction-configuration 1

Entry number: 1
Reaction Configuration not configured

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip sla reaction-configuration 1
Router(config)# do show ip sla reaction-configuration 1

Entry number: 1
Reaction: rtt
Threshold Type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: None
```

Verifying an IP SLAs Reaction Configuration: Example

In the following example, multiple monitored elements (indicated by the `Reaction:` value) are configured for a single IP SLAs operation:

```
Router# show ip sla reaction-configuration

Entry Number: 1
Reaction: RTT
Threshold type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: None

Reaction: jitterDSAvg
Threshold type: average
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: triggerOnly

Reaction: jitterDSAvg
Threshold type: immediate
Rising (milliseconds): 5
Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly

Reaction: PacketLossSD
Threshold type: immediate
Rising (milliseconds): 5
Threshold Falling (milliseconds): 3
Threshold Count: 5
Threshold Count2: 5
Action Type: trapOnly
```

Table 1 describes the significant fields shown in this output.

Table 1 *show ip sla reaction-configuration Field Descriptions*

Field	Description
Reaction	The configured monitored element for IP SLAs reactions. Corresponds to the react { connectionLoss jitterAvg jitterDSAvg jitterSDAvg mos PacketLossDS PacketLossSD rtt timeout verifyError } syntax in the ip sla reaction-configuration command.
Threshold type	The configured threshold type. Corresponds to the threshold-type { never immediate consecutive xofy average } syntax in the ip sla reaction-configuration command.
Rising (milliseconds)	The <i>upper-threshold</i> value, as configured by the threshold-value upper-threshold lower-threshold syntax in the ip sla reaction-configuration command.
Threshold Falling (milliseconds)	The <i>lower-threshold</i> value, as configured by the threshold-value upper-threshold lower-threshold syntax in the ip sla reaction-configuration command.
Threshold Count	The <i>x-value</i> in the xofy threshold-type, or the <i>number-of-probes</i> value for average threshold-type.
Threshold Count2	The <i>y-value</i> in the xofy threshold-type.
Action Type	The reaction to be performed when the violation conditions are met, as configured by the action-type { none trapOnly triggerOnly trapAndTrigger } syntax in the ip sla reaction-configuration command.

Triggering SNMP Notifications: Example

In the following example, CISCO-SYSLOG-MIB traps will be sent to the remote host at 209.165.202.129 if the threshold values for round-trip-time (rtt) or VoIP mean opinion score (MOS) are violated:

```
Router(config)# ip sla 1
Router(config-ip-sla)# udp-jitter 209.165.200.225 3000 codec g711alaw
Router(config-ip-sla-jitter)# default frequency
Router(config-ip-sla-jitter)# exit

Router(config)# ip sla schedule 1 start now life forever
Router(config)# ip sla reaction-configuration 1 react rtt threshold-type immediate
threshold-value 3000 2000 action-type trapOnly
Router(config)# ip sla reaction-configuration 1 react MOS threshold-type consecutive 4
threshold-value 390 220 action-type trapOnly

Router(config)# ip sla logging traps
Router(config)#
Router(config)# snmp-server host 209.165.202.129 version 2c public syslog
! The following command is needed for the system to generate CISCO-SYSLOG-MIB traps.
```

```
Router(config)# snmp-server enable traps syslog
```

As shown in the following example, the IP SLAs Threshold violations are generated as level 6 (informational) in the Cisco IOS system logging process:

```
3d18h:%RTT-6-SAATHRESHOLD:RTR(11):Threshold exceeded for MOS
```

but are sent as level 7 (info) notifications from the CISCO-SYSLOG-MIB:

```
3d18h:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 32613038
snmpTrapOID.0 = ciscoSyslogMIB.2.0.1
clogHistoryEntry.2.71 = RTT
clogHistoryEntry.3.71 = 7
clogHistoryEntry.4.71 = SAATHRESHOLD
clogHistoryEntry.5.71 = RTR(11):Threshold exceeded for MOS
clogHistoryEntry.6.71 = 32613037
```

Where to Go Next

For information about other types of IP SLAs operations and IP SLAs features, see the [Cisco IOS IP SLAs Features Roadmap](#).

Additional References

The following sections provide references related to configuring Cisco IOS IP SLAs.

Related Documents

Related Topic	Document Title
Cisco IOS IP SLAs command-line interface enhancements	Cisco IOS IP Service Level Agreements Command Line Interface , Cisco white paper
Cisco IOS IP SLAs commands	Cisco IOS IP SLAs Command Reference

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by features in this document.	—

MIBs

MIBs	MIBs Link
CISCO-RTTMON-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No specific RFCs are supported by the features in this document.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Feature Information for IP SLAs Proactive Threshold Monitoring

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information for IP SLAs Proactive Threshold Monitoring

Feature Name	Releases	Feature Information
IP SLAs Reaction Threshold	12.3(14)T, 12.2(31)SB2, 12.2(33)SRB1, 12.2(33)SXH, Cisco IOS XE Release 2.1	Cisco IOS IP SLAs proactive threshold monitoring capability allows you to configure an IP SLAs operation to react to certain measured network conditions.
IP SLAs VoIP Threshold Traps	12.3(14)T, 12.2(31)SB2, 12.2(33)SRB1, 12.2(33)SXH, Cisco IOS XE Release 2.1	Cisco IOS IP SLAs VoIP proactive threshold monitoring capability allows you to configure an IP SLAs operation to react to certain measured network conditions.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006-2008 Cisco Systems, Inc. All rights reserved.

