IP SLAs Reaction Threshold

Feature History for IP SLAs - Reaction Threshold

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 17.18.1	IP SLAs - Reaction Threshold: This feature monitors a specified value or event and intiates a trigger when the defined threshold is exceeded or when a specific event, such as a timeout or connection loss occurs.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

IP SLAs reaction

IP SLA reactions are configured to trigger when a monitored value exceeds or falls below a specified threshold, or when a specific event occurs, such as a timeout or connection loss. If an IP SLA operation detects that a monitored value is either too high or too low according to its configured reactions, it can generate a notification to a network management application or initiate another IP SLA operation to collect additional data.

When an IP SLA operation is triggered, the target operation begins and runs independently, without awareness of the status of the original triggering operation. The target operation will continue to run until a

condition-cleared event occurs. After this event, the target operation stops gracefully, and its state changes from Active to Pending, allowing it to be triggered again.

Supported reactions by IP SLAs operation

The tables below list which reactions are supported for each IP SLA operation.

Table 1: Supported Reaction Configuration, by IP SLA Operation

Reaction	ICMP Echo	Path Echo	UDP Jitter	UDP Echo	TCP Connect	DHCP	DLSW	ICMP Jitter	DNS	Frame Relay
Failure	Y	--	Y	Y	Y	Y	--	Y	Y	--
RTT	Y	Y	--	Y	Y	Y	Y	--	Y	Y
RTTAvg	--	--	Y	--	--	--	--	Y	--	--
timeout	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
connectionLoss	--	--	Y	Y	Y	--	--	--	--	
verifyError	--	--	Y	Y	--	--	--	Y	--	Y
jitterSDAvg	--	--	Y	--	--	--		Y	--	--
jitterAvg	--	--	Y	--	--	--	--	Y	--	--
packetLateArrival	--	--	Y	--	--	--	--	Y	--	--
packetOutOfSequence	--	--	Y	--	--	--	--	Y	--	--
MaxOfPostiveSD	--	--	Y	--	--	--		Y	--	--
MaxOfNegativeSD	--	--	Y	--	--	--	--	Y	--	--
MaxOfPostiveDS	--	--	Y	--	--	--	--	Y	--	--
MaxOfNegativeDS	--	--	Y	--	--	--	--	Y	--	--
MOS	--	--	Y	--	--	--		--	--	--
ICPIF	--	--	Y	--	--	--	--	--	--	--
PacketLossDS	--	--	Y	--	--	--	--	--	--	--
PacketLossSD	--	--	Y	--	--	--	--	--	--	--
PacketMIA	--	--	Y	--	--	--		--	--	--
iaJitterDS	--	--	--	--	--	--	--	--	--	--
frameLossDS	--	--	--	--	--	--	--	--	--	--
mosLQDSS	--	--	--	--	--	--	--	--	--	--

Reaction	ICMP Echo	Path Echo	UDP Jitter	UDP Echo	TCP Connect	DHCP	DLSW	ICMP Jitter	DNS	Frame Relay
mosCQDS	--	--	--	--	--	--	--	--	--	--
rfactorDS	--	--	--	--	--	--	--	--	--	--
iaJitterSD	--	--	--	--	--	--	--	--	--	--
successivePacketLoss	--	--	--	--	--	--	--	Y	--	--
MaxOfLatencyDS	--	--	--	--	--	--	--	Y	--	--
MaxOfLatencySD	--	--	--	--	--	--	--	Y	--	--
LatencyDS	--	--	--	--	--	--	--	Y	--	--
LatencySD	--	--	--	--	--	--	--	Y	--	--
packetLoss	--	--	--	--	--	--	--	Y	--	--

Table 2: Supported Reaction Configuration, by IP SLA Operation

Reaction	HTTP	SLM	RTP	FTP	Lsp Trace	Post delay	Path Jitter	LSP Ping	Gatekeeper Registration
Failure	--	--	--	--	--	--	--	--	--
RTT	Y	Y	Y	Y	Y	Y	Y	Y	Y
RTTAvg	--	--	--	--	--	--	--	--	--
timeout	Y	Y	Y	Y	--	Y	Y	Y	Y
connectionLoss	Y		Y	Y	Y	--	--	Y	--
verifyError	--	--	--	--	--	--	--	--	--
jitterSDAvg	--	--	--	--	--	--	Y	--	--
jitterAvg	--	--	--	--	--	--	Y	--	--
packetLateArrival	--	--	--	--	--	--	Y	--	--
packetOutOfSequence	--	--	--	--	--	--	Y	--	--
MaxOfPostiveSD	--	--	--	--	--	--	Y	--	--
MaxOfNegativeSD	--	--	--	--	--	--	Y	--	--
MaxOfPostiveDS	--	--	--	--	--	--	Y	--	--
MaxOfNegativeDS	--	--	--	--	--	--	Y	--	--
MOS	--	--	--	--	--	--	--	--	--

Reaction	HTTP	SLM	RTP	FTP	Lsp Trace	Post delay	Path Jitter	LSP Ping	Gatekeeper Registration
ICPIF	--	--	--	--	--	--	--	--	--
PacketLossDS	--	--	Y	--	--	--	--	--	--
PacketLossSD	--	--	Y	--	--	--	--	--	--
PacketMIA	--	--	Y	--	--	--	--	--	--
iaJitterDS	--	--	Y	--	--	--	--	--	--
frameLossDS	--	--	Y	--	--	--	--	--	--
mosLQDSS	--	--	Y	--	--	--	--	--	--
mosCQDS	--	--	Y	--	--	--	--	--	--
rfactorDS	--	--	Y						
iaJitterSD	--	--	Y	--	--	--	--	--	--
successivePacketLoss	--	--	--	--	--	--	--	--	--
MaxOfLatencyDS	--	--	--	--	--	--	--	--	--
MaxOfLatencySD	--	--	--	--	--	--	--	--	--
LatencyDS	--	--	--	--	--	--	--	--	--
LatencySD	--	--	--	--	--	--	--	--	--
packetLoss	--	--	--	--	--	--	--	--	--

IP SLAs reaction threshold monitoring and notifications

IP SLAs support proactive threshold monitoring and notifications for performance parameters such as average jitter, unidirectional latency, bidirectional round-trip time (RTT), and connectivity across most IP SLA operations. This proactive monitoring capability also enables the configuration of reaction thresholds for key VoIP-related parameters, including unidirectional jitter, unidirectional packet loss, and unidirectional VoIP voice quality scoring.

Notifications for IP SLAs are configured as triggered reactions. Packet loss, jitter, and Mean Opinion Score (MOS) statistics are specific to IP SLA jitter operations. Notifications can be generated for threshold violations in either direction—source-to-destination or destination-to-source—or for out-of-range RTT values related to packet loss and jitter. Events such as traps are triggered when the RTT value exceeds or falls below a specified threshold.

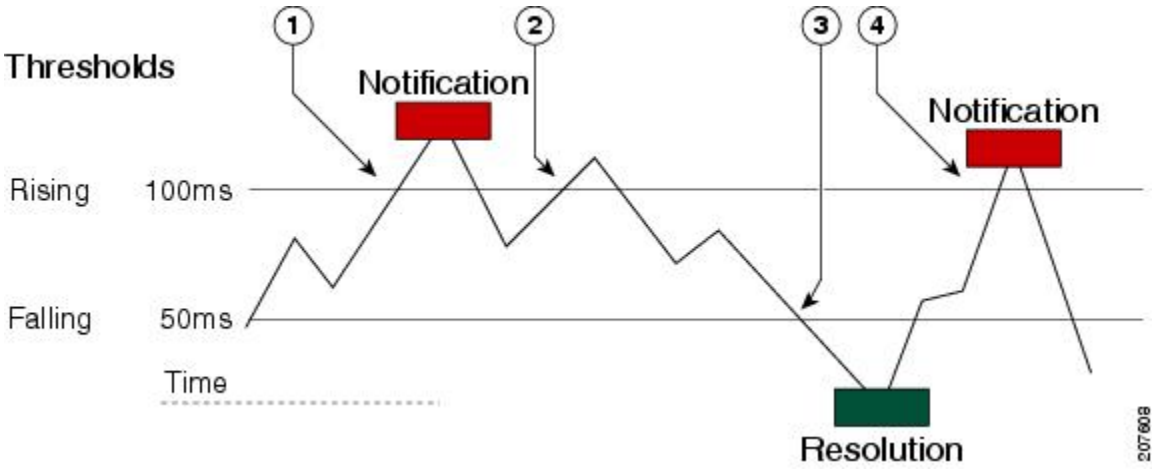
IP SLAs can generate system logging (syslog) messages when a reaction condition occurs. These syslog messages can also be sent as Simple Network Management Protocol (SNMP) traps (notifications) using the CISCO-RTTMON-MIB. SNMP traps for IP SLAs are supported by both the CISCO-RTTMON-MIB and the CISCO-SYSLOG-MIB.

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

IP SLA threshold violations are logged as level 6 (informational) within the Cisco system logging process, but are sent as level 7 (info) traps from the CISCO-SYSLOG-MIB.

Notifications are not issued for every occurrence of a threshold violation. The process works as follows: when the monitored element exceeds the upper (rising) threshold for the first time, an event is sent and a notification is issued. Subsequent notifications are only generated after the monitored value falls below the lower (falling) threshold and then exceeds the upper threshold again.

Figure 1: IP SLAs triggered teaction condition and notifications for threshold exceeded



1	An event is sent and a threshold-exceeded notification is issued when the rising threshold is exceeded for the first time.
2	Consecutive over-rising threshold violations occur without issuing additional notifications.
3	Themonitored value goes below the falling threshold.
4	Another threshold-exceeded notification is issued when the rising threshold is exceeded only after the monitored value first fell below the falling threshold.

Note A lower-threshold notification is also issued the first time the monitored element falls below the falling threshold. As described, subsequent notifications for lower-threshold violations are only generated after the monitored value first exceeds the rising threshold and then falls below the falling threshold again.

RTT Reactions for jitter operations

RTT reactions for jitter operations are triggered only at the end of the operation and use the most recent value for return-trip time (LatestRTT), which is equal to the average return-trip time (RTTAvg).

SNMP traps for RTT in jitter operations are based on the average return-trip time (RTTAvg) for the entire operation and do not include RTT values for individual packets sent during the operation. For example, if the average RTT is below the threshold, it is possible for up to half of the packets to have RTT values above the threshold. However, this detail is not reflected in the notification, as only the overall average is reported.

Only syslog messages are supported for RTTAvg threshold violations. These syslog messages are sent from the CISCO-RTTMON-MIB.

Guidelines to configure reaction threshold

- RTT reactions for jitter operations are triggered only at the end of the operation and use the latest value for the return-trip time (LatestRTT).
- SNMP traps for RTT for jitter operations are based on the average value for the return-trip time (RTTAvg) for the whole operation only and do not include return-trip time values for individual packets sent during the operation. Only syslog messages are supported for RTTAvg threshold violations.
- Only syslog messages are supported for RTT violations during Jitter operations.
- Only SNMP traps are supported for RTT violations during non-Jitter operations.
- Only syslog messages are supported for non-RTT violations other than timeout, connectionLoss, or verifyError.
- Both SNMP traps and syslog messages are supported for timeout, connectionLoss, or verifyError violations only

Configure IP SLAs Reaction Threshold

Before you begin

IP SLAs operations to be started when violation conditions are met must be configured.

Perform this task to configure thresholds and reactive triggering for generating traps or starting another operation.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **ip sla reaction-configuration** *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]

Example:

```
Device(config)# ip sla reaction-configuration 10 react jitterAvg threshold-type immediate
threshold-value 5000 3000 action-type trapAndTrigger
```

Configures the action (SNMP trap or IP SLAs trigger) that is to occur based on violations of specified thresholds.

- *operation-number*: The number of the IP SLA operation to which the reaction will be applied.
- *monitored-element*: The specific parameter to monitor (e.g., rtt, jitter, packet-loss).
- **action-type** *option*: The action to take when the threshold is crossed (optional, e.g., trapOnly, triggerOnly, trapAndTrigger).
- **threshold-type**: The method for evaluating the threshold. Options include:
  - **average** *number-of-measurements*: Triggers based on the average over a specified number of measurements.
  - **consecutive** *occurrences*: Triggers after a specified number of consecutive occurrences.
  - **immediate**: Triggers immediately when the threshold is crossed.
  - **never**: Disables reactions.
  - **xofy** [*x-value y-value*]: Triggers when x out of y occurrences exceed the threshold.
  - **threshold-value** *upper-threshold lower-threshold*: Specifies the upper and lower threshold values for the monitored element.

Step 4 **ip sla reaction-trigger** *operation-number target-operations*

Example:

```
Device(config)# ip sla reaction-trigger 10 2
```

(Optional) Starts another IP SLAs operation when the violation conditions are met.

This command is required only if the **ip sla reaction-configuration** command is configured with either the **trapAndTrigger** or **triggerOnly** keyword.

Step 5 **ip sla logging traps**

Example:

```
Device(config)# ip sla logging traps
```

(Optional) Enables IP SLAs syslog messages from CISCO-RTTMON-MIB.

Step 6 Configure one of the following:

- **snmp-server enable traps rtr**
- **snmp-server enable traps syslog**

Example:

```
Device(config)# snmp-server enable traps rtr
OR
Device(config)# snmp-server enable traps syslog
```

Enables the system to generate SNMP traps.

The first example shows how to enable the system to generate CISCO-RTTMON-MIB. The second example shows how to enable the system to generate CISCO-SYSLOG-MIB traps.

Step 7 **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]

Example:

```
Device(config)# snmp-server host 10.1.1.1 public syslog
```

(Optional) Sends traps to a remote host.

Required if the **snmp-server enable traps** command is configured.

Step 8 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode and returns to privileged EXEC mode.

Step 9 **show ip sla reaction-configuration** [*operation-number*]

Example:

```
Device# show ip sla reaction-configuration 10
```

(Optional) Displays the configuration of proactive threshold monitoring.

Step 10 **show ip sla reaction-trigger** [*operation-number*]

Example:

```
Device# show ip sla reaction-trigger 2
```

(Optional) Displays the configuration status and operational state of target operations to be triggered.

Configuration examples for IP SLAs reaction threshold

The following example shows how to configure IP SLAS reaction threshold using the **ip sla reaction-configuration** command. In this example, IP SLAs operation 10 is configured to send an SNMP logging trap when the MOS value either exceeds 4.9 (best quality) or falls below 2.5 (poor quality):

```
Device> enable
Device# configure terminal
Device(config)# ip sla reaction-configuration 10 react mos threshold-type immediate
threshold-value 490 250 action-type trapOnly
```

The following example is a sample output of the **show ip sla reaction-configuration** command.

```
Device# show ip sla reaction-configuration 1
Entry number: 1
Reaction Configuration not configured
```

The following example show the default configuration of the **ip sla reaction-configuration** command.

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

The following example shows that multiple monitored elements are configured for the IP SLAs operation (1), as indicated by the values of Reaction: in the output:

```
Device# 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
```

The following example shows how to configure IP SLAs reaction threshold so that CISCO-SYSLOG-MIB traps are sent to the remote host at 10.1.1.1 if the threshold values for RTT or VoIP MOS are violated:

```
! Configure the operation on source.
Device(config)# ip sla 1
Device(config-ip-sla)# udp-jitter 10.1.1.1 3000 codec g711alaw
Device(config-ip-sla-jitter)# exit
Device(config)# ip sla schedule 1 start now life forever
! Configure thresholds and reactions.
Device(config)# ip sla reaction-configuration 1 react rtt threshold-type immediate
threshold-value 3000 2000 action-type trapOnly
Device(config)# ip sla reaction-configuration 1 react MOS threshold-type consecutive 4
threshold-value 390 220 action-type trapOnly
Device(config)# ip sla logging traps
```

```
! The following command sends traps to the specified remote host.
Device(config)# snmp-server host 10.1.1.1 version 2c public syslog
! The following command is needed for the system to generate CISCO-SYSLOG-MIB traps.
Device(config)# snmp-server enable traps syslog
```

The following sample system logging messages shows that IP SLAs threshold violation notifications are generated as level 6 (informational) in the Cisco system logging process:

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

This following sample SNMP notification from the CISCO-SYSLOG-MIB for the same violation is a level 7 (info) notification:

```
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
```