Configuring Proactive Threshold Monitoring for IP SLAs Operations

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

This chapter includes the following sections:

Information About IP SLAs Reaction Configuration

IP SLAs reactions are configured to trigger when a monitored value exceeds or falls below a specified level or when a monitored event, such as a timeout or connection loss, occurs. If IP SLAs measure too high or too low of any configured reaction, IP SLAs can generate a notification to a network management application or trigger another IP SLA operation to gather more data.

IP SLAs 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 for most IP SLAs operations. The proactive monitoring capability also provides options for configuring reaction thresholds for important VoIP related parameters including unidirectional jitter, unidirectional packet loss, and unidirectional VoIP voice quality scoring.

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

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

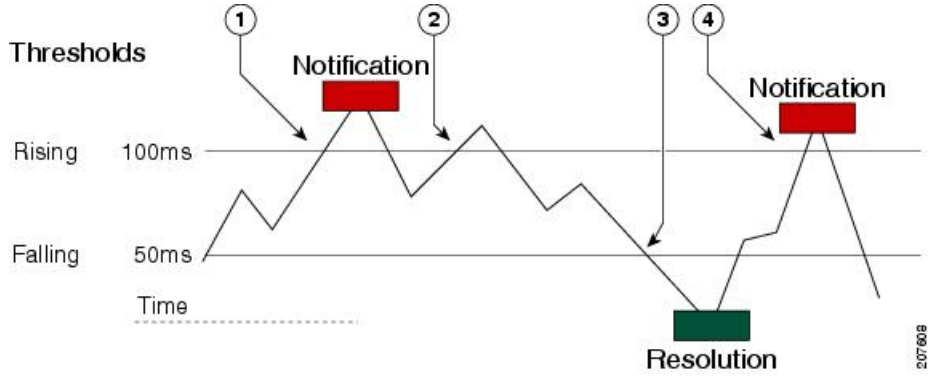
Severity levels in the CISCO-SYSLOG-MIB are SyslogSeverity INTEGER {emergency(1), alert(2), critical(3), error(4), warning(5), notice(6), info(7), debug(8)}.

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

IP SLAs threshold violations are logged as level 6 (informational) within the Cisco NX-OS 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 following figure shows the sequence for a triggered reaction that occurs when the monitored element exceeds the upper threshold. An event is sent and a notification is issued when the rising threshold is exceeded for the first time. Subsequent threshold-exceeded notifications are issued only after the monitored value falls below the falling threshold before exceeding the rising threshold again.

Figure 1: IP SLAs Triggered Reaction 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	The monitored 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 that the monitored element falls below the falling threshold (3). Subsequent notifications for lower-threshold violations are issued only after the rising threshold is exceeded before the monitored value 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 latest value for the return-trip time (LatestRTT), which matches the value of the average return-trip time (RTTAvg).

SNMP traps for RTT for jitter operations are based on the value of the average return-trip time (RTTAvg) for the whole operation and do not include RTT values for each individual packet sent during the operation. For example, if the average is below the threshold, up to half of the packets can actually be above the threshold, but this detail is not included in the notification because the value is for the whole operation only.

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

Configuring Proactive Threshold Monitoring

This section describes how to configure thresholds and reactive triggering for generating traps or starting another operation.

Before you begin

- Configure IP SLAs operations to be started when violation conditions are met.

Note

- 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 nonjitter 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.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`switch# configure terminal`	
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-valuey-value*]}] [**threshold-value** *upper-thresholdlower-threshold*] **Example:** `switch(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.
Step 4	**ip sla reaction-trigger** *operation-number target-operation* **Example:** `switch(config)# ip sla reaction-trigger 10 2`	(Optional) Starts another IP SLAs operation when the violation conditions are met. 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:** `switch(config)# ip sla logging traps`	(Optional) Enables IP SLAs syslog messages from CISCO-RTTMON-MIB.
Step 6	**snmp-server enable traps ip sla** **Example:** `switch(config)# snmp-server enable traps ip sla`	(Optional) Enables system to generate CISCO-RTTMON-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:** `switch(config)# snmp-server host 10.1.1.1 public`	(Optional) Sends traps to a remote host. Required if the **snmp-server enable traps** command is configured.
Step 8	**exit** **Example:** `switch(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 9	**show ip sla reaction configuration** [*operation-number*] **Example:**	(Optional) Displays the configuration of proactive threshold monitoring.

	Command or Action	Purpose
	`switch# show ip sla reaction configuration 10`	
Step 10	**show ip sla reaction trigger** [*operation-number*] **Example:** `switch# show ip sla reaction trigger 2`	(Optional) Displays the configuration status and operational state of target operations to be triggered.

Configuration Example for an IP SLAs Reaction Configuration

This example shows how to configure IP SLAs operation 10 to send an SNMP logging trap when the MOS value either exceeds 4.9 (best quality) or falls below 2.5 (poor quality):

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

This example shows how to display the default configuration:

```
switch# show ip sla reaction-configuration 1
Entry number: 1
Index: 1
Reaction: mos
Threshold Type: Immediate
Rising: 490
Falling: 250
Action Type: Trap only
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip sla reaction-configuration 10 react mos threshold-type immediate
threshold-value 490 250 action-type trapOnly
switch(config)# 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
```

Verification Example for an IP SLAs Reaction Configuration

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

```
switch# 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
```

Configuration Example for Triggering SNMP Notifications

This example shows how to configure proactive threshold monitoring 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.
switch(config)# ip sla 1

switch(config-ip-sla)# udp-jitter 10.1.1.1 3000 codec g711alaw
switch(config-ip-sla-jitter)# exit

switch(config)# ip sla schedule 1 start now life forever

! Configure thresholds and reactions.
switch(config)# ip sla reaction-configuration 1 react rtt threshold-type immediate
threshold-value 3000 2000 action-type trapOnly

switch(config)# ip sla reaction-configuration 1 react MOS threshold-type consecutive 4
threshold-value 390 220 action-type trapOnly

switch(config)# ip sla logging traps

! The following command sends traps to the specified remote host.
switch(config)# snmp-server host 10.1.1.1 version 2c public

! The following command is needed for the system to generate CISCO-SYSLOG-MIB traps.
switch(config)# snmp-server enable traps
```

This example shows that IP SLAs threshold violation notifications are generated as level 6 (informational) in the Cisco NX-OS system logging process:

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

This example shows an 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
```