R through Se

react (tplt-icmp-ech)

To configure reaction and proactive threshold monitoring parameters in an auto IP Service Level Agreements (SLAs) operation template for an Internet Control Message Protocol (ICMP) echo operation, use the **react** command in the ICMP echo submode of IP SLA template configuration mode. To disable all threshold monitoring or to disable individual monitored elements, use the **no** form of this command.

react [*monitored-element* [[**action-type** *type-of-action*] [**threshold-type** {**average** [*number-of-measurements*]| **consecutive** [*occurrences*]| **immediate**| **never**| **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]]]

no react [*monitored-element*]

Syntax Description

monitored-element	(Optional) Element to be monitored for threshold violations. Valid keywords are: • **timeout** --Reaction should occur if there is a one-way timeout. • **verifyError** --Reaction should occur if there is a one-way error verification violation • **rtt** --Reaction should occur if round-trip time violates upper or lower threshold.
action-type	(Optional) Specifies action to be taken when threshold violations occur.
type-of-action	(Optional) Keywords for*type-of-action* are: • **none** --No action is taken when threshold violations occur. This keyword combination is default for RTT. • **trapOnly** --A Simple Network Management Protocol (SNMP) trap notification should be sent when the specified violation type occurs for the monitored element. **Note** If the **threshold-typenever** keywords are configured, the **action-type***type-of-action* keyword and argument combination is disabled.
threshold-type average	(Optional) Specifies that the reaction occurs when the average of a specified number of measurements for the monitored element either exceeds the *upperthreshold* or drops below the *lowerthreshold*.

number-of-measurement	(Optional) Number of averaged measurements. Range is 1 to 16. Default is 5. For example, if the *number-of-measurement* for **threshold-typeaverage** is 3 and the upper threshold is 5000 ms and the last three results of the operation are 6000, 6000, and 5000 ms, the average would be 6000 + 6000 + 5000 = 17000/3 = 5667 ms and the average exceeds the upper threshold of 5000 ms.
threshold-type consecutive	(Optional) Specifies that the reaction occurs when threshold violation is consecutively met for a specified number of times.
occurrences	(Optional) Number of consecutive occurrences. Range is 1 to 16. Default is 5.
threshold-type immediate	(Optional) Specifies that the reaction occurs each time the threshold violation is met.
threshold-type never	(Optional) Specifies that threshold violations should not be monitored. This is the default threshold type. **Note** If these keywords are configured, the **action-typenone** and **action-typetrapOnly** keywords are disabled.
threshold-type xofy	(Optional) Specifies that the reaction occurs when violation threshold for the monitored element is met x number of times within the last y number of measurements.
x-value y-value	(Optional) Range for the x-value and for the y-value is 1 to 16. Default is 5 for both values.
threshold-value	(Optional) Specifies upper-threshold and lower-threshold values for monitored elements
upper-threshold	Value in milliseconds. For defaults, see the table below.
lower-threshold	Value in milliseconds. For defaults, see the table below.

Command Default IP SLAs proactive threshold monitoring is disabled.

Command Modes ICMP echo submode of IP SLA template configuration (config-tplt-icmp-ech)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command enables proactive threshold monitoring for one or more elements in the auto IP SLAs operation template being configured and defines the conditions under which the operation makes the transition from pending to active.

You can configure this command multiple times so as to allow reactions for multiple monitored elements.

The **noformof** this command with one or more keywords can be used to disable individual monitored elements or use the **noreact** command without keywords to disable all proactive threshold monitoring in the auto IP SLAs operation template.

The table below lists the default upper and lower thresholds for specific monitored elements.

Table 1: Default Threshold Values for Monitored Elements

Monitored Element Keyword	Upper Threshold	Lower Threshold
rtt	5000 ms	3000 ms

Only SNMP traps are supported for round-trip time (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.

SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB and CISCO-SYSLOG-MIB. Use the **ipslaloggingtraps** command to enable the generation of SNMP system logging messages specific to IP SLAs trap notifications. Use the **snmp-serverenabletrapsrtr** or **snmp-serverenabletrapssyslog**command to enable the sending of IP SLAs SNMP trap notifications.

To display the current threshold monitoring configuration for an auto IP SLAs operation, use the **showipslaautotemplate**command.

Examples

The following example shows how to configure operation parameters and proactive threshold monitoring using an auto IP SLAs operation template. In this example, the proactive threshold monitoring configuration for the ICMP echo operation specifies that when three consecutive timeout events occur, an SNMP trap notification should be sent.

```
Router(config)#ip sla auto template type ip icmp-echo react-to

Router(config-tplt-icmp-ech)#react timeout action-type traponly threshold-type conecutive
3
Router(config-tplt-icmp-ech)#end
Router# show ip sla auto template type ip icmp-echo
IP SLAs Auto Template: react-to
    Measure Type: icmp-echo
    Description:
```

```
    .
.
.
Reaction Configuration:
       Reaction Index       : 1
         Reaction           : timeout
         Threshold Type     : Consecutive
         Threshold CountX   : 3
         Threshold CountY   : 5
         Action Type        : Trap Only
```

Related Commands

Command	Description
ip sla logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
show ip sla auto template	Displays configuration including default values of auto IP SLAs operation templates.
snmp-server enable traps rtr	Enables system to generate CISCO-RTTMON-MIB traps.
snmp-server enable traps syslog	Enables system to generate CISCO-SYSLOG-MIB traps.

react (tplt-icmp-jtr)

To configure reaction and proactive threshold monitoring parameters in an auto IP Service Level Agreements (SLAs) operation template for an Internet Control Message Protocol (ICMP) jitter operation, use the **react** command in the ICMP jitter submode of IP SLA template configuration mode. To disable all threshold monitoring or to disable individual monitored elements, use the **no** form of this command.

react [*monitored-element* [[**action-type** *type-of-action*] [**threshold-type** {**average** [*number-of-measurements*]| **consecutive** [*occurrences*]| **immediate**| **never**| **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]]]

no react [*monitored-element*]

Syntax Description

monitored-element	(Optional) Element to be monitored for threshold violations. Valid keywords are: • **jitterAvg** --Reaction should occur if the average round-trip jitter value violates the upper threshold or lower threshold. • **jitterDSAvg** --Reaction should occur if the average one-way destination-to-source jitter value violates the upper threshold or lower threshold. • **jitterSDAvg** --Reaction should occur if the average one-way source-to-destination jitter value violates the upper threshold or lower threshold. • **latencyDSAvg** --Reaction should occur if the average one-way destination-to-source latency value violates the upper threshold or lower threshold. • **latencySDAvg** --Reaction should occur if the average one-way source-to-destination latency value violates the upper threshold or lower threshold. • **maxOfLatencyDS** --Reaction should occur if the one-way maximum destination-to-source latency value is violated. • maxOfLatencySD--Reaction should occur if the one-way maximum source-to-destination latency value is violated. • **maxOfNegativeDS** --Reaction should occur if the one-way maximum negative jitter destination-to-source threshold is violated. • **maxOfNegativeSD** --Reaction should occur if the one-way maximum negative jitter source-to-destination threshold is violated. • **maxOfPositiveDS** --Reaction should occur if the one-way maximum positive jitter destination-to-source threshold is violated. • **maxOfPositiveSD** --Reaction should occur if the one-way maximum positive jitter source-to-destination threshold is violated.

monitored-element (continued)	• **packetLateArrival** --Reaction should occur if the one-way number of late packets violates the upper threshold or lower threshold. • **packetLoss** --Reaction should occur if the packet loss value violates the upper threshold or lower threshold. The path of the packets is either destination-to-source or source-to-destination. • **packetOutOfSequence** --Reaction should occur if the one-way number of packets out of sequence violates the upper threshold or lower threshold. • **rtt** --Reaction should occur if the round-trip time (RTT) violates the upper threshold or lower threshold. • **successivePacketLoss** • **timeout** --Reaction should occur if there is a one-way timeout for the monitored operation. The **threshold-value** keyword does not apply to this monitored element. • **verifyError** --Reaction should occur if there is a one-way error verification violation. The **threshold-value** keyword does not apply to this monitored element.
action-type *type-of-action*	(Optional) Specifies action to be taken when threshold violations occur. Keywords for*type-of-action* are: • **none** --No action is taken when threshold violations occur. This keyword combination is default for RTT. • **trapOnly** --A Simple Network Management Protocol (SNMP) trap notification should be sent when the specified violation type occurs for the monitored element. **Note** If the **threshold-typenever** keywords are configured, the **action-type***type-of-action* keyword and argument combination is disabled.
threshold-type average	(Optional) Specifies that the reaction occurs when the average of a specified number of measurements for the monitored element either exceeds the *upperthreshold* or drops below the *lowerthreshold*.

number-of-measurement	(Optional) Number of averaged measurements. Range is 1 to 16. Default is 5. For example, if the *number-of-measurement* value for **threshold-typeaverage** is 3 and the upper threshold is 5000 ms and the last three results of the operation are 6000, 6000, and 5000 ms, the average would be 6000 + 6000 + 5000 = 17000/3 = 5667 ms and the average exceeds the upper threshold of 5000 ms.
threshold-type consecutive	(Optional) Specifies that the reaction occurs when threshold violation is consecutively met for a specified number of times.
occurrences	(Optional) Number of consecutive occurrences. Range is 1 to 16. Default is 5.
threshold-type immediate	(Optional) Specifies that the reaction occurs each time the threshold violation is met.
threshold-type never	(Optional) Specifies that threshold violations should not be monitored. This is the default threshold type. **Note** If these keywords are configured, the **action-typenone** and **action-typetrapOnly** keywords are disabled.
threshold-type xofy	(Optional) Specifies that the reaction occurs when threshold violation for the monitored element is met *x* number of times within the last *y* number of measurements.
x-value y-value	Range for the x-value and for the y-value is 1 to 16. Default is 5 for both values.
threshold-value	(Optional) Specifies upper-threshold and lower-threshold values for monitored elements
upper-threshold	(Optional) Value in milliseconds (ms). For defaults, see the table below.
lower-threshold	(Optional) Value in milliseconds (ms). For defaults, see the table below.

Command Default IP SLAs proactive threshold monitoring is disabled.

Command Modes ICMP jitter submode of IP SLA template configuration (config-tplt-icmp-jtr)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command enables proactive threshold monitoring for one or more elements in the auto IP SLAs operation template being configured and defines the conditions under which the operation makes the transition from pending to active.

You can configure this command multiple times so as to allow reactions for multiple monitored elements.

The **no**form of this command with one or more keywords can be used to disable individual monitored elements or use the **no** form of this command without keywords to disable all proactive threshold monitoring in the auto IP SLAs operation template.

Return-trip time (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.

For Mean opinion score (MOS), values are computed as numbers to two decimal places, from a value of 1.00 (worst quality) to 5.00 (best quality). The number for *upper-threshold* and *lower-threshold* is expressed in three digits representing ones, tenths, and hundredths. For example, to express a MOS threshold of 3.20, enter **320**. The valid range is from 100 (1.00) to 500 (5.00).

The table below lists the default upper and lower thresholds for specific monitored elements.

Table 2: Default Threshold Values for Monitored Elements

Monitored Element Keyword	Upper Threshold	Lower Threshold
icpif	93 (score)	93 (score)
jitterAvg	100 ms	100 ms
jitterDSAvg	100 ms	100 ms
jitterSDAvg	100 ms	100 ms
latencyDSAvg	5000 ms	3000 ms
latencySDAvg	5000 ms	3000 ms
maxOflatencyDS	5000 ms	3000 ms
maxOflatencySD	5000 ms	3000 ms
maxOfNegativeDS	10000 ms	10000 ms

Monitored Element Keyword	Upper Threshold	Lower Threshold
maxOfNegativeSD	10000 ms	10000 ms
maxOfPositiveDS	10000 ms	10000 ms
maxOfPositiveSD	10000 ms	10000 ms
mos	500 (score)	100 (score)
packetLateArrival	10000 packets	10000 packets
packetLossDS	10000 packets	10000 packets
packetLossSD	10000 packets	10000 packets
packetMIA	10000 packets	10000 packets
packetOutOfSequence	10000 packets	10000 packets
rtt	5000 ms	3000 ms

Only syslog messages are supported for RTTAvg threshold violations.

Only syslog messages are supported for RTT violations during 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.

SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB and CISCO-SYSLOG-MIB.

Use the **snmp-serverenabletrapsrtr** or **snmp-serverenabletrapssyslog**command to enable the sending of IP SLAs SNMP trap notifications.

Use the **ipslaloggingtraps** command to enable the generation of SNMP system logging messages specific to IP SLAs trap notifications. Only system logging messages are supported for RTTAvg threshold violations.

To display the current threshold monitoring configuration settings for an auto IP SLAs operation, use the **showipslaautotemplate**command.

Examples

The following example shows how to configure operation parameters and proactive threshold monitoring using an auto IP SLAs operation template. In this example, the proactive threshold monitoring configuration for the ICMP jitter operation specifies that when three consecutive packet loss events occur, an SNMP trap notification should be sent:

```
Router(config)#ip sla auto template type ip icmp-jitter react-closs

Router(config-tplt-icmp-jtr)#react packetloss action-type traponly threshold-type conecutive
 3
Router(config-tplt-icmp-jtr)#end
Router# show ip sla auto template type ip icmp-jitter
IIP SLAs Auto Template: react
    Measure Type: icmp-jitter
```

```
   .
.
.
Reaction Configuration:
       Reaction Index       : 1
         Reaction           : packetLoss
         Threshold Type     : Consecutive
         Threshold Rising   : 3
         Threshold Falling  : 10000
         Threshold CountX   : 3
         Threshold CountY   : 5
         Action Type        : Trap Only
```

Related Commands

Command	Description
ip sla logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
show ip sla auto template	Displays configuration including default values of auto for IP SLAs a operation templates.
snmp-server enable traps rtr	Enables system to generate CISCO-RTTMON-MIB traps.
snmp-server enable traps syslog	Enables system to generate CISCO-SYSLOG-MIB traps.

react (tplt-tcp-conn)

To configure reaction and proactive threshold monitoring parameters in an auto IP Service Level Agreements (SLAs) operation template for an Transmission Control Protocol (TCP) connect operation, use the **react** command in the TCP connect submode of IP SLA template configuration mode. To disable all threshold monitoring or to disable individual monitored elements, use the **no** form of this command.

react [*monitored-element* [[**action-type** *type-of-action*] [**threshold-type** {**average** [*number-of-measurements*]| **consecutive** [*occurrences*]| **immediate**| **never**| **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]]]

no react [*monitored-element*]

Syntax Description

monitored-element	(Optional) Element to be monitored for threshold violations. Valid keywords are: • **connectionLoss** --Reaction should occur if there is a one-way connection loss for the monitored operation. The **threshold-value**keyword does not apply to this monitored element. • **rtt** --Reaction should occur if the round-trip time (RTT) violates the upper threshold or lower threshold. • **timeout** --Reaction should occur if there is a one-way timeout for the monitored operation. The **threshold-value** keyword does not apply to this monitored element.
action-type *type-of-action*	(Optional) Specifies action to be taken when threshold violations occur. Keywords for*type-of-action* are: • **none** --No action is taken when threshold violations occur. This keyword combination is default for RTT. • **trapOnly** --A Simple Network Management Protocol (SNMP) trap notification should be sent when the specified violation type occurs for the monitored element. **Note** If the **threshold-typenever** keywords are configured, the **action-type***type-of-action* keyword and argument combination is disabled.

threshold-type average	(Optional) Specifies that the reaction occurs when the average of a specified number of measurements for the monitored element either exceeds the *upperthreshold* value or drops below the *lowerthreshold*value.
number-of-measurement	(Optional) Number of averaged measurements. Range is 1 to 16. Default is 5. For example, if the *number-of-measurement* value for **threshold-typeaverage** is 3 and the upper threshold is 5000 ms and the last three results of the operation are 6000, 6000, and 5000 ms, the average would be 6000 + 6000 + 5000 = 17000/3 = 5667 ms and the average exceeds the upper threshold of 5000 ms.
threshold-type consecutive	(Optional) Specifies that the reaction occurs when threshold violation is consecutively met for a specified number of times.
occurrences	(Optional) Number of consecutive occurrences. Range is 1 to 16. Default is 5.
threshold-type immediate	(Optional) Specifies that the reaction occurs each time the threshold violation is met.
threshold-type never	(Optional) Threshold violations should not be monitored. This is the default threshold type. **Note** If the **threshold-typenever** keywords are configured, the **action-typenone** and **action-typetrapOnly** keywords are disabled.
threshold-type xofy	(Optional) Specifies that the reaction occurs when threshold violation for the monitored element is met *x* number of times within the last *y* number of measurements.
x-value y-value	Range for the x-value and for the y-value is 1 to 16. Default is 5 for both values.
threshold-value	(Optional) Specifies upper-threshold and lower-threshold values for monitored elements
upper-threshold	(Optional) Value in milliseconds (ms). For defaults, see the table below.
lower-threshold	(Optional) Value in milliseconds (ms). For defaults, see the table below.

Command Default IP SLAs proactive threshold monitoring is disabled.

Command Modes TCP connect submode of IP SLA template configuration (config-tplt-tcp-conn)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines This command enables proactive threshold monitoring for one or more elements in the auto IP SLAs operation template being configured and defines the conditions under which the operation makes the transition from pending to active.

You can configure this command multiple times so as to allow reactions for multiple monitored elements.

The **no** form of this command with one or more keywords can be used to disable individual monitored elements or use the **no** form of this command without keywords to disable all proactive threshold monitoring in the auto IP SLAs operation template.

The table below lists the default upper and lower thresholds for specific monitored elements.

Table 3: Default Threshold Values for Monitored Elements

Monitored Element Keyword	Upper Threshold	Lower Threshold
rtt	5000 ms	3000 ms

Only SNMP traps are supported for return-trip time (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.

SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB and CISCO-SYSLOG-MIB. Use the **ipslaloggingtraps** command to enable the generation of SNMP system logging messages specific to IP SLAs trap notifications. Use the **snmp-serverenabletrapsrtr** or **snmp-serverenabletrapssyslog**command to enable the sending of IP SLAs SNMP trap notifications.

To display the current threshold monitoring configuration settings for an auto IP SLAs operation, use the **showipslaautotemplate**command.

Examples The following example shows how to configure operation parameters and proactive threshold monitoring using an auto IP SLAs operation template. In this example, the proactive threshold monitoring configuration for the TCP connect operation specifies that when three timeout connection loss events occur, an SNMP trap notification should be sent:

```
Router(config)#ip sla auto template type ip tcp-connect react-to
```

```
Router(config-tplt-tcp-conn)#react timout action-type traponly threshold-type conecutive 3
Router(config-tplt-tcp-conn)#end
Router# show ip sla auto template type ip tcp-connect
IP SLAs Auto Template: react-to
    Measure Type: tcp-connect
    Description:
    .
 .
 .
 Reaction Configuration:
        Reaction Index       : 1
          Reaction           : timeout
          Threshold Type     : Consecutive
          Threshold CountX   : 3
          Threshold CountY   : 5
          Action Type        : Trap Only
```

Related Commands

Command	Description
ip sla logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
show ip sla auto template	Displays configuration including default values of auto IP SLAs operation templates.
snmp-server enable traps rtr	Enables system to generate CISCO-RTTMON-MIB traps.
snmp-server enable traps syslog	Enables system to generate CISCO-SYSLOG-MIB traps.

react (tplt-udp-ech)

To configure reaction and proactive threshold monitoring parameters in an auto IP Service Level Agreements (SLAs) operation template for a User Datagram Protocol (UDP) echo operation, use the **react** command in the UDP echo submode of IP SLA template configuration mode. To disable all threshold monitoring or to disable individual monitored elements, use the **no** form of this command.

react [*monitored-element* [[**action-type** *type-of-action*] [**threshold-type** {**average** [*number-of-measurements*]| **consecutive** [*occurrences*]| **immediate**| **never**| **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]]]

no react [*monitored-element*]

Syntax Description

monitored-element	(Optional) Element to be monitored for threshold violations. Valid keywords are: • **connectionLoss** --Reaction should occur if there is a one-way connection loss for the monitored operation. The **threshold-value**keyword does not apply to this monitored element. • **rtt** --Reaction should occur if the round-trip time (RTT) violates the upper threshold or lower threshold. • **timeout** --Reaction should occur if there is a one-way timeout for the monitored operation. The **threshold-value** keyword does not apply to this monitored element. • **verifyError** --Reaction should occur if there is a one-way error verification violation. The **threshold-value** keyword does not apply to this monitored element.
action-type *type-of-action*	(Optional) Specifies action to be taken when threshold violations occur. Valid keywords are: • **none** --No action is taken when threshold violations occur. This keyword combination is default for RTT. • **trapOnly** --A Simple Network Management Protocol (SNMP) trap notification should be sent when the specified violation type occurs for the monitored element. **Note** If the **threshold-typenever** keywords are configured, the **action-type***type-of-action* keyword and argument combination is disabled.

threshold-type average	(Optional) Specifies that the reaction occurs when the average of a specified number of measurements for the monitored element either exceeds the *upperthreshold* or drops below the *lowerthreshold*.
number-of-measurement	(Optional) Number of averaged measurements. Range is 1 to 16. Default is 5. For example, if the *number-of-measurement* value for **threshold-typeaverage** is 3 and the upper threshold is 5000 ms and the last three results of the operation are 6000, 6000, and 5000 ms, the average would be 6000 + 6000 + 5000 = 17000/3 = 5667 ms and the average exceeds the upper threshold of 5000 ms.
threshold-type consecutive	(Optional) Specifies that the reaction occurs when threshold violation is consecutively met for a specified number of times.
occurrences	(Optional) Number of consecutive occurrences. Range is 1 to 16. Default is 5.
threshold-type immediate	(Optional) Specifies that the reaction occurs each time the threshold violation is met.
threshold-type never	(Optional) Specifies that threshold violations should not be monitored. This is the default threshold type. **Note** If the **threshold-typenever** keywords are configured, the **action-typenone** and **action-typetrapOnly** keywords are disabled.
threshold-type xofy	(Optional) Specifies that the reaction occurs when threshold violation for the monitored element is met *x* number of times within the last *y* number of measurements.
x-value y-value	Range for the x-value and for the y-value is 1 to 16. Default is 5 for both values.
threshold-value	(Optional) Specifies upper-threshold and lower-threshold values for monitored elements
upper-threshold	(Optional) Value in milliseconds (ms). For defaults, see the table below.
lower-threshold	(Optional) Value in milliseconds (ms). For defaults, see the table below.

Command Default IP SLAs proactive threshold monitoring is disabled.

Command Modes UDP echo submode of IP SLA template configuration (config-tplt-udp-ech)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines This command enables proactive threshold monitoring for one or more elements in the auto IP SLAs operation template being configured and defines the conditions under which the operation makes the transition from pending to active.

You can configure this command multiple times to allow reactions for multiple monitored elements.

The **no**form of this command with one or more keywords can be used to disable individual monitored elements or use the **no** form of this command without keywords to disable all proactive threshold monitoring in the auto IP SLAs operation template.

The table below lists the default upper and lower thresholds for specific monitored elements.

Table 4: Default Threshold Values for Monitored Elements

Monitored Element Keyword	Upper Threshold	Lower Threshold
rtt	5000 ms	3000 ms

Only SNMP traps are supported for round-trip time (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.

SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB and CISCO-SYSLOG-MIB. Use the **ipslaloggingtraps** command to enable the generation of SNMP system logging messages specific to IP SLAs trap notifications. Use the **snmp-serverenabletrapsrtr** or **snmp-serverenabletrapssyslog**command to enable the sending of IP SLAs SNMP trap notifications.

To display the current threshold monitoring configuration settings for an auto IP SLAs operation, use the **showipslaautotemplate**command.

Examples The following example shows how to configure operation parameters and proactive threshold monitoring using an auto IP SLAs operation template. In this example, the proactive threshold monitoring configuration for the UDP echo operation specifies that when three consecutive timeout events occur, an SNMP trap notification is sent:

```
Router(config)#ip sla auto template type ip udp-echo react-to
```

```
Router(config-tplt-udp-ech)#react timeout action-type traponly threshold-type conecutive 3
Router(config-tplt-udp-ech)#end
Router# show ip sla auto template type ip udp-echo
IP SLAs Auto Template: react-to
    Measure Type: udp-echo
    Description:
    .
 .
 .
 Reaction Configuration:
        Reaction Index       : 1
          Reaction           : timeout
          Threshold Type     : Consecutive
          Threshold CountX   : 3
          Threshold CountY   : 5
          Action Type        : Trap Only
```

Related Commands

Command	Description
ip sla logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
show ip sla auto template	Displays configuration including default values of auto IP SLAs operation templates.
snmp-server enable traps rtr	Enables system to generate CISCO-RTTMON-MIB traps.
snmp-server enable traps syslog	Enables system to generate CISCO-SYSLOG-MIB traps.

react (tplt-udp-jtr)

To configure reaction and proactive threshold monitoring parameters in an auto IP Service Level Agreements (SLAs) operation template for an User Datagram Protocol (UDP) jitter operation, use the **react** command in the UDP jitter submode of IP SLA template configuration mode. To disable all threshold monitoring or to disable individual monitored elements, use the **no** form of this command.

react [*monitored-element* [[**action-type** *type-of-action*] [**threshold-type** {**average** [*number-of-measurements*]| **consecutive** [*occurrences*]| **immediate**| **never**| **xofy** [*x-value y-value*]}] [**threshold-value** *upper-threshold lower-threshold*]]]

no react [*monitored-element*]

Syntax Description

monitored-element	

(Optional) Element to be monitored for threshold violations. Valid keywords are:

- **connectionLoss** --Reaction should occur if there is a one-way connection loss for the monitored operation. The **threshold-value**keyword does not apply to this monitored element.
- **icpif** --Calculated Planning Impairment Factor.
- **jitterAvg** --Reaction should occur if the average round-trip jitter value violates the upper threshold or lower threshold.
- **jitterDSAvg** --Reaction should occur if the average one-way destination-to-source jitter value violates the upper threshold or lower threshold.
- **jitterSDAvg** --Reaction should occur if the average one-way source-to-destination jitter value violates the upper threshold or lower threshold.
- **latencyDSAvg** --Reaction should occur if the average one-way destination-to-source latency value violates the upper threshold or lower threshold.
- **latencySDAvg** --Reaction should occur if the average one-way source-to-destination latency value violates the upper threshold or lower threshold.
- **maxOfLatencyDS** --Reaction should occur if the one-way maximum destination-to-source latency value is violated.
- maxOfLatencySD--Reaction should occur if the one-way maximum source-to-destination latency value is violated.
- **maxOfNegativeDS** --Reaction should occur if the one-way maximum negative jitter destination-to-source threshold is violated.
- **maxOfNegativeSD** --Reaction should occur if the one-way maximum negative jitter source-to-destination threshold is violated.
- **maxOfPositiveDS** --Reaction should occur if the one-way maximum positive jitter destination-to-source threshold is violated.
- **maxOfPositiveSD** --Reaction should occur if the one-way maximum positive jitter

	source-to-destination threshold is violated.
monitored-element (continued)	• **mos** --Mean Opinion Score (mos) in either direction rises above or falls below a specified threshold. • **packetLateArrival** --Reaction should occur if the one-way number of late packets violates the upper threshold or lower threshold. • **packetLossDS** --Reaction should occur if the packet loss value violates the upper threshold or lower threshold. The path of the packets is unknown. • **packetLossSD** --Reaction should occur if the packet loss value violates the upper threshold or lower threshold. The path of the packets is unknown. • **packetMIA** --Reaction should occur if the packetis not returned. • **packetOutOfSequence** --Reaction should occur if the one-way number of packets out of sequence violates the upper threshold or lower threshold. • **rtt** --Reaction should occur if the round-trip time (RTT) violates the upper threshold or lower threshold. • **timeout** --Reaction should occur if there is a one-way timeout for the monitored operation. The **threshold-value** keyword does not apply to this monitored element. • **verifyError** --Reaction should occur if there is a one-way error verification violation. The **threshold-value** keyword does not apply to this monitored element.

action-type *type-of-action*	(Optional) Specifies action to be taken when threshold violations occur. Valid keywords are: • **none** --No action is taken when threshold violations occur. This keyword combination is default for RTT. • **trapOnly** --A Simple Network Management Protocol (SNMP) trap notification should be sent when the specified violation type occurs for the monitored element. **Note** If the **threshold-typenever** keywords are configured, the **action-type***type-of-action* keyword and argument combination is disabled.
threshold-type average	(Optional) Specifies that the reaction occurs when the average of a specified number of measurements for the monitored element either exceeds the *upperthreshold* or drops below the *lowerthreshold*.
number-of-measurement	(Optional) Number of averaged measurements. Range is 1 to 16. Default is 5. For example, if the *number-of-measurement* value for **threshold-typeaverage** is 3 and the upper threshold is 5000 ms and the last three results of the operation are 6000, 6000, and 5000 ms, the average would be 6000 + 6000 + 5000 = 17000/3 = 5667 ms and the average exceeds the upper threshold of 5000 ms.
threshold-type consecutive	(Optional) Specifies that the reaction occurs when threshold violation is consecutively met for a specified number of times.
occurrences	(Optional) Number of consecutive occurrences. Range is 1 to 16. Default is 5.
threshold-type immediate	(Optional) Specifies that the reaction occurs each time the threshold violation is met.
threshold-type never	(Optional) Specifies that threshold violations should not be monitored. This is the default threshold type. **Note** If these keywords are configured, the **action-typenone** and **action-typetrapOnly** keywords are disabled.

threshold-type xofy	(Optional) Specifies that the reaction occurs when threshold violation for the monitored element is met *x* number of times within the last *y* number of measurements.
x-value y-value	(Optional) Range for the x-value and for the y-value is 1 to 16. Default is 5 for both values.
threshold-value	(Optional) Specifies upper-threshold and lower-threshold values for monitored elements
upper-threshold	Value in milliseconds (ms). For defaults, see the table in the Usage Guidelines section.
lower-threshold	Value in milliseconds (ms). For defaults, see the table in the Usage Guidelines section.

Command Default

IP SLAs proactive threshold monitoring is disabled.

Command Modes

UDP jitter submode of IP SLA template configuration (config-tplt-udp-jtr)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command enables proactive threshold monitoring for one or more elements in the auto IP SLAs operation template being configured and defines the conditions under which the operation makes the transition from pending to active.

You can configure this command multiple times so as to allow reactions for multiple monitored elements.

The **no**form of this command with one or more keywords can be used to disable individual monitored elements or use the **noreact** command without keywords to disable all proactive threshold monitoring in the auto IP SLAs operation template.

Return-trip time (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.

For Mean opinion score (MOS), values are computed as numbers to two decimal places, from a value of 1.00 (worst quality) to 5.00 (best quality). The numbers for *upper-threshold* and *lower-threshold* arguments are expressed in three digits representing ones, tenths, and hundredths. For example, to express a MOS threshold of 3.20, enter **320**. The valid range is from 100 (1.00) to 500 (5.00).

The table below lists the default upper and lower thresholds for specific monitored elements.

Table 5: Default Threshold Values for Monitored Elements

Monitored Element Keyword	Upper Threshold	Lower Threshold
icpif	93 (score)	93 (score)
jitterAvg	100 ms	100 ms
jitterDSAvg	100 ms	100 ms
jitterSDAvg	100 ms	100 ms
latencyDSAvg	5000 ms	3000 ms
latencySDAvg	5000 ms	3000 ms
maxOflatencyDS	5000 ms	3000 ms
maxOflatencySD	5000 ms	3000 ms
maxOfNegativeDS	10000 ms	10000 ms
maxOfNegativeSD	10000 ms	10000 ms
maxOfPositiveDS	10000 ms	10000 ms
maxOfPositiveSD	10000 ms	10000 ms
mos	500 (score)	100 (score)
packetLateArrival	10000 packets	10000 packets
packetLossDS	10000 packets	10000 packets
packetLossSD	10000 packets	10000 packets
packetMIA	10000 packets	10000 packets
packetOutOfSequence	10000 packets	10000 packets
rtt	5000 ms	3000 ms

Only syslog messages are supported for RTTAvg threshold violations.

Only syslog messages are supported for RTT violations during 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.

SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB and CISCO-SYSLOG-MIB.

Use the **snmp-serverenabletrapsrtr** or **snmp-serverenabletrapssyslog**command to enable the sending of IP SLAs SNMP trap notifications.

Use the **ipslaloggingtraps** command to enable the generation of SNMP system logging messages specific to IP SLAs trap notifications. Only system logging messages are supported for RTTAvg threshold violations.

To display the current threshold monitoring configuration settings for an auto IP SLAs operation, use the **showipslaautotemplate**command.

Examples

The following example shows how to configure operation parameters and proactive threshold monitoring using an auto IP SLAs operation template. In this example, the proactive threshold monitoring configuration for the UDP jitter operation specifies that when three consecutive timeout events occur, an SNMP trap notification should be sent:

```
Router(config)#ip sla auto template type ip udp-jitter react-to

Router(config-tplt-udp-jtr)#react timeout action-type traponly threshold-type conecutive 3
Router(config-tplt-udp-jtr)#end
Router# show ip sla auto template type ip udp-jitter
IP SLAs Auto Template: react-to
    Measure Type: udp-jitter
    Description:
    .
 .
 .
 Reaction Configuration:
        Reaction Index       : 1
          Reaction           : timeout
          Threshold Type     : Consecutive
          Threshold CountX   : 3
          Threshold CountY   : 5
          Action Type        : Trap Only
```

Related Commands

Command	Description
ip sla logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
show ip sla auto template	Displays configuration including default values of auto IP SLAs operation templates.
snmp-server enable traps rtr	Enables system to generate CISCO-RTTMON-MIB traps.
snmp-server enable traps syslog	Enables system to generate CISCO-SYSLOG-MIB traps.

reply-dscp-bits

To specify the differentiated services codepoint (DSCP) value for an echo reply packet of a Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation, use the **reply-dscp-bits** command in auto IP SLA MPLS parameters configuration mode. To return to the default value, use the **no** form of this command.

reply-dscp-bits *dscp-value*

no reply-dscp-bits *dscp-value*

Syntax Description

dscp-value	Specifies the differentiated services codepoint (DSCP) value for an echo reply packet.

Command Default

The DSCP value is 0.

Command Modes

Auto IP SLA MPLS parameters configuration (config-auto-ip-sla-mpls-params)

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

You must configure the type of LSP Health Monitor operation (such as LSP ping) before you can configure any of the other parameters of the operation.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing and forwarding (VRF) instances associated with the source Provider

Edge (PE) router. The DSCP value for the echo reply packets of IP SLAs operations created by LSP Health Monitor operation 1 is set to 5.

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 timeout 1000
 scan-interval 1
 secondary-frequency connection-loss 10
 secondary-frequency timeout 10
 delete-scan-factor 2
 reply-dscp-bits 5
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive
 3 action-type trapOnly
ip sla logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.

reply-mode

To specify the reply mode for an echo request packet of a Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation, use the **reply-mode** command in auto IP SLA MPLS parameters configuration mode. To return to the default value, use the **no** form of this command.

reply-mode {**ipv4**| **router-alert**}

no reply-mode {**ipv4**| **router-alert**}

Syntax Description

ipv4	Replies with an IPv4 User Datagram Protocol (UDP) packet (default).
router-alert	Replies with an IPv4 UDP packet with router alert.

Command Default

The reply mode for an echo request packet is an IPv4 UDP packet by default.

Command Modes

Auto IP SLA MPLS parameters configuration (config-auto-ip-sla-mpls-params)

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

You must configure the type of LSP Health Monitor operation (such as LSP ping) before you can configure any of the other parameters of the operation.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing and forwarding (VRF) instances associated with the source Provider

Edge (PE) router. The reply mode of an echo request packet for IP SLAs operations created by LSP Health Monitor operation 1 is an IPv4 UDP packet with router alert.

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 timeout 1000
 scan-interval 1
 secondary-frequency connection-loss 10
 secondary-frequency timeout 10
 delete-scan-factor 2
 reply-mode router-alert
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive
 3 action-type trapOnly
ip sla logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.

request-data-size

To set the protocol data size in the payload of a Cisco IOS IP Service Level Agreements (SLAs) operation's request packet, use the **request-data-size**command in the appropriate submode of IP SLA configuration, auto IP SLA MPLS configuration, IP SLA monitor configuration, or IP SLA template parameters configuration mode. To return to the default value, use the **no** form of this command.

request-data-size *bytes*

no request-data-size

Syntax Description

bytes	Size of the protocol data in the payload of the request packet of the operation, in bytes. Range is from 0 to the maximum supported by the protocol.

Command Default

The default data size varies depending on the type of IP SLAs operation you are configuring. See the CISCO-RTTMON-MIB documentation for more details.

Command Modes

DLSw configuration (config-ip-sla-dlsw) ICMP echo configuration (config-ip-sla-echo) ICMP path echo configuration (config-ip-sla-pathEcho) ICMP path jitter configuration (config-ip-sla-pathJitter) UDP echo configuration (config-ip-sla-udp) UDP jitter configuration (config-ip-sla-jitter) VCCV configuration (config-sla-vccv)

Command Modes

MPLS parameters configuration (config-auto-ip-sla-mpls-params)

Command Modes

DLSw configuration (config-sla-monitor-dlsw) ICMP echo configuration (config-sla-monitor-echo) ICMP path echo configuration (config-sla-monitor-pathEcho) ICMP path jitter configuration (config-sla-monitor-pathJitter) UDP echo configuration (config-sla-monitor-udp) UDP jitter configuration (config-sla-monitor-jitter)

Command Modes

ICMP echo configuration (config-icmp-ech-params) UDP echo configuration (config-udp-ech-params) UDP jitter configuration (config-icmp-ech-params)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	The VCCV configuration mode was added.
12.2(33)SB	The VCCV configuration mode was added.
15.1(1)T	This command was modified. The IP SLA template-parameters configuration mode was added.

Usage Guidelines

The **request-data-size** command can be used to set the padding size for the data frame of an IP SLAs Ethernet operation. See the documentation for the **request-data-size** (Ethernet) command for more information.

The **request-data-size** command is supported in IPv4 networks. This command is also supported in IPv6 networks to configure an IP SLAs operation that supports IPv6 addresses.

IP SLAs Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see the Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release table). If you are configuring an IP SLAs label switched path (LSP) Health Monitor operation, see the Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release table for information on Cisco IOS release dependencies. You must configure the type of IP SLAs operation, such as User Datagram Protocol (UDP) jitter or Internet Control Message Protocol (ICMP) echo, before you can configure any of the other parameters of the operation.

The configuration mode for the **request-data-size** command varies depending on the Cisco IOS release you are running and the operation type configured.

If you are running Cisco IOS IP SLAs Engine 3.0, you must enter the **parameters** command in IP SLA template configuration mode before you can use the **request-datasize** command.

Table 6: Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(4)T, 12.0(32)SY, 12.2(33)SRB, 12.2(33)SB, 12.2(33)SXI, or later releases	**ip sla**	IP SLA configuration
12.3(14)T, 12.4, 12.4(2)T, 12.2(31)SB2, or 12.2(33)SXH	**ip sla monitor**	IP SLA monitor configuration

Table 7: Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(6)T, 12.0(32)SY, 12.2(31)SB2, 12.2(33)SRB, 12.2(33)SXH, or later releases	**auto ip sla mpls-lsp-monitor**	Auto IP SLA MPLS configuration
15.1(1)T	ip sla auto template	IP SLA template configuration

Examples

The following examples show how to set the request packet size to 40 bytes for an IP SLAs ICMP echo operation. Note that the Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see the Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release table).

Examples

```
ip sla 3
 icmp-echo 172.16.1.175
 request-data-size 40
!
ip sla schedule 3 life forever start-time now
```

Examples

```
ip sla monitor 3
 type echo protocol ipIcmpEcho 172.16.1.175
 request-data-size 40
!
ip sla monitor schedule 3 life forever start-time now
```

Examples

```
Router(config)# ip sla auto template type ip icmp-echo 1
Router(config-icmp-ech-tplt)# parameters
Router(config-icmp-ech-params)# request-data-size 40
Router(config-icmp-ech-params)# end
Router#
Router# show ip sla auto template type ip icmp-echo
IP SLAs Auto Template: 1
Measure Type: icmp-echo (control enabled)
    Description:
    IP options:
        Source IP: 0.0.0.0      Source Port: 0
        VRF:    TOS: 0x0
    Operation Parameters:
        Request Data Size: 40 Verify Data: false
  Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    History options:
        History filter: none
        Max number of history records kept: 15
        Lives of history kept: 0
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla auto template	Begins configuration for an auto IP SLAs operation template and enters IP SLA template configuration mode.
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.

request-data-size (Ethernet)

To set the padding size for the data frame of a Cisco IOS IP Service Level Agreements (SLAs) Ethernet operation, use the **request-data-size** (Ethernet) command in the appropriate submode of IP SLA configuration or auto IP SLA MPLS configuration mode. To return to the default value, use the **no** form of this command.

request-data-size *bytes*

no request-data-size

Syntax Description

bytes	Padding size (in bytes) for the data frame of the operation. The range is from 0 to the maximum of the protocol.

Command Default

The default padding size will vary depending on the type of IP SLAs operation you are configuring. See the CISCO-RTTMON-MIB documentation for more details.

Command Modes

Ethernet echo (config-ip-sla-ethernet-echo)

Ethernet jitter (config-ip-sla-ethernet-jitter)

Command Modes

Ethernet parameters configuration (config-ip-sla-ethernet-params)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

You must configure the type of Ethernet operation (such as Ethernet ping) before you can configure any of the other parameters of the operation.

Examples

The following example shows how to set the padding size to 40 bytes for IP SLAs Ethernet ping operation 3:

```
ip sla 3
 ethernet echo mpid 23 domain testdomain vlan 34
 request-data-size 40
!
ip sla schedule 3 life forever start-time now
```

Related Commands

Command	Description
auto ip sla ethernet-monitor	Begins configuration for an IP SLAs auto Ethernet operation and enters IP SLA Ethernet monitor configuration mode.
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

reserve dsp

To reserve digital signalling processing (DSP) credits for an IP Service Level Agreements (SLAs) video operation from the previously reserved DSP video services pool, use the **reserve dsp** command in IP SLA video configuration mode. To return to the default, use the **no** form of this command.

reserve dsp

no reserve dsp

Syntax Description

This command has no arguments or keywords.

Command Default

No DSP resources are explicitly reserved for IP SLAs video operations and video services are deployed on a best-effort basis.

Command Modes

IP SLA video configuration (config-ip-sla-video)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use the **reserve dsp** command to reserve DSP resources for IP SLAs video operations.

Video resources are allocated when the operation is initiated and then released when the operation has completed. During the operation's times pan, it is guaranteed that each session of this operation will be serviced by reserved resources. If resources are not reserved for IP video services, video services are deployed on a best-effort basis; that is, each session will attempt to allocate DSP resources when the session starts at the scheduled time.

Before DSP resources can be allocated to IP SLAs video operations, a percentage of the total voice and video DSP resources, or credits, must be first allocated to the video DSP resource pool to be used for all types of video operations. Allocate DSP resources to the DSP resource pool using the **voice-service dsp-reservation** command.

Examples

```
Router(config-ip-sla-video)# reserve dsp
Router(config-ip-sla-video)#
```

Related Commands

Command	Description
voice-service dsp-reservation	Specifies the percentage of DSP resources that are reserved strictly for VOIP on the voice card.

resolution

To configure the resolution parameter in a user-defined video traffic profile for an IP Service Level Agreements (SLAs) video operation, use the **resolution** command in the appropriate IP SLA VO profile endpoint configuration submode. To remove the resolution value, use the **no** form of this command.

resolution *resolution*

no resolution *resolution*

Syntax Description

resolution	Resolution for profile being configured in pixels. The following keywords are valid options for the resolution: • **QCIF**: The resolution is 176 x 144 and is valid for the CP-9900 and custom video endpoint types only. • **QVCA**: The resolution is 320 x 240 and is valid for only the custom video endpoint type. • **SIF**: The resolution is 352 x 240 and is valid for only the custom video endpoint type. • **CIF**: The resolution is 352 x 288 and is vaid for the CP-9900 and custom video endpoint types. • **VGA**: The resolution is 640 x 480 and is valid for the CP-9900 and custom video endpoint types. • **4CIF**: The resoluiton is 704 x 480 (also used for w448) and is valid for only the custom video endpoint type. • **4SIF**: The resoluiton is 704 x 480 and is valid for only the custom video endpoint type. • **720P**: The resoluiton is 1280 x 720 and is valid for the CTS and custom video endpoint types. • **1080P**: The resoluiton is 1920 x 1080 and is valid for the CTS and custom video endpoint types. For a description of each traffic profile type, see the "Usage Guidelines" section.

Command Default

No resolution is specified in the video profile.

Command Modes

IP SLA VO CP9900 profile endpoint configuration (cfg-ipslavo-cp9900-profile)

IP SLA VO CTS profile endpoint configuration (cfg-ipslavo-cts-profile)

IP SLA VO custom profile endpoint configuration (cfg-ipslavo-custom-profile)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use the **resolution** command to configure the resolution parameter in a video profile for the following video endpoint types:

- CP-9900—Cisco Unified 9900 Series IP Phone System (CP-9900).
- CTS—Cisco Telepresence System 1000/3000 (CTS-1000/3000)
- custom—Customized video endpoint type.

The keywords for this command are not case sensitive. The keywords in online help contain uppercase letters to enhance readability only.

There are restrictions based on the relationships between maximum bit rate, frame rate, and resolution, also known as bandwidth. For the user-defined endpoint types, the table below includes the maximum bit rates allowable in relation to the frame per second (fps) rates and resolution. Cisco IOS software allows you to enter the values of these three parameters in any order and verifies that their combination is within a valid range, as specified. For example, if a 1080 pixels (p) resolution at 30 fps is chosen, the valid maximum bit-rate range is between 1500 and 4000 kb/s.

Table 8: Maximum Bit Rates Allowable for Frame Rates and Resolution in Custom Endpoints

Resolution and Frame Rate	30/24 fps	15 fps	10 fps	7.5 fps	5 fps
QCIF	60–256 kb/s	32–160 kb/s	20–118 kb/s	15–96 kb/s	10–74 kb/s
CIF/SIG/QVGA	128–1000 kb/s	64–564 kb/s	43–397 kb/s	32–314 kb/s	22–230 kb/s
VGA/4CIF/4SIF	384–2000 kb/s	192–1128 kb/s	128–795 kb/s	96–628 kb/s	64–461 kb/s
720p	800–2500 kb/s	400–1506 kb/s	267–1089 kb/s	200–881 kb/s	133–673 kb/s
1080p	1500–4000 kb/s	750–2512 kb/s	500–1845 kb/s	375–1512 kb/s	250–1179 kb/s

Press **Shift+?** to display only those options that are applicable for various endpoint type configurations. For example, if CTS is the previously configured endpoint type, the only resolutions available are 720p and 1080p.

Examples

```
Router> enable
Router# configure terminal
Router(config)# ip sla profile video my-profile
Router(cfg-ipslavo-profile)# endpoint custom
Router(cfg-ipslavo-custom-profile)# resolution VGA
```

Related Commands

Command	Description
bitrate (VO profile)	Configures the max bit rate or bit-rate window size parameter in a user-defined video profile.
frame	Configures frame parameters in a user-defined video profile.
show ip sla profile video	Displays a summary of IP SLAs video traffic profiles.

response-data-size

To set the protocol data size in the payload of a Cisco IOS IP Service Level Agreements (SLAs) operation response packet, use the **response-data-size** command in UDP jitter configuration mode. To return to the default value of the protocol data size in the payload of the response packet, use the **no** form of this command.

response-data-size *bytes*

no response-data-size

Syntax Description

bytes	Size of the protocol data in the payload of a response packet, in bytes. The range is from 21 to the maximum size supported by the UDP protocol.

Command Default

The default response data size varies depending on the type of IP SLAs operation configured.

Command Modes

UDP jitter configuration (config-ip-sla-jitter)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

The **response-data-size** command enables Cisco IP SLAs to support custom-defined packet sizes based on the direction (sender to receiver and receiver to sender) of the traffic. This command is supported in IPv4 and IPv6 networks to configure an IP SLAs operation.

Note If the **response-data-size** command is not configured, then the response data size value is the same as the request data size value.

Examples

The following example shows how to set the response data size to 25 bytes for an IP SLAs UDP jitter operation:

```
Device> enable
Device# configure terminal
Device(config)# ip sla 10
Device(config-ip-sla)# udp-jitter 192.0.2.114 55
Device(config-ip-sla-jitter)# response-data-size 25
Device(config-ip-sla-jitter)# end
```

Related Commands

Command	Description
ip sla	Starts configuring an IP SLAs operation and enters IP SLA configuration mode.
udp-jitter	Configures an IP SLAs UDP jitter operation.

rtp (VO profile)

To configure the Real-time Transport Protocol (RTP) parameters in a user-defined custom video traffic profile for an IP Service Level Agreements (SLAs) video operation, use the **rtp** command in IP SLA VO custom profile endpoint configuration submode. To return the default, use the **no** form of this command.

rtp {**size average** *avg-size*| **buffer output** {**burst**| **shaped**}}

no rtp {**size average** *avg-size*| **buffer output** {**burst**| **shaped**}}

Syntax Description

size average *avg-size*	Specifies the synthetic video RTP average size in bytes. The range is from 500 to 1300. The default is 1000.
buffer output	Specifies that the synthetic video RTP buffer accepts output packet transmissions. This is the default.
bursty	Specifies that the synthetic video RTP buffer accepts bursty output. This is the default.
shaped	Specifies that the synthetic video RTP buffer accepts shaped output.

Command Default

The RTP average size is 1000 bytes and the synthetic video RTP buffer accepts bursty output.

Command Modes

IP SLA VO custom profile endpoint configuration (cfg-ipslavo-custom-profile)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use this command to change the values for the RTP parameters in a user-defined custom video traffic profile from the defaults (1000 bytes and bursty output) to the specified values. The RTP packet is the carrier vehicle for video media traffic.

Bursty output is defined as sending packets immediately after they are ready for transmission. Shaped output is defined as sending packets evenly distributed within a frame interval.

Examples

```
Router> enable
Router# configure terminal
Router(config)# ip sla profile video my-profile
Router(cfg-ipslavo-profile)# endpoint cts
Router(cfg-ipslavo-cts-profile)# rtp size average 800
```

```
Router(cfg-ipslavo-cts-profile)# rtp buffer output shaped
```

Related Commands

Command	Description
show ip sla profile video	Displays a summary of IP SLAs video traffic profiles.

rtr

Note Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr**command is replaced by the **ip sla monitor**command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr**command is replaced by the **ip sla**command. See the **ip sla monitor**and **ip sla**commands for more information.

To begin configuration for a Cisco IOS IP Service Level Agreements (IP SLAs) operation and enter RTR configuration mode, use the **rtr**command in global configuration mode. To remove all configuration information for an operation, including the schedule of the operation, reaction configuration, and reaction triggers, use the no form of this command.

rtr *operation-number*

no rtr *operation-number*

Syntax Description

operation-number	Operation number used for the identification of the IP SLAs operation you wish to configure.

Command Default

No IP SLAs operation is configured.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(11)T	The maximum number of operations was increased from 500 to 2000 (SAA Engine II).
12.3(14)T	This command was replaced by the **ip sla monitor** command.
12.2(31)SB2	This command was replaced by the **ip sla monitor** command.
12.2(33)SRB	This command was replaced by the **ip sla**command.

Usage Guidelines

The **rtr** command is used to configure Cisco IOS IP Service Level Agreements (IP SLAs) operations. Use this command to specify an identification number for the operation you are about to configure. After you enter this command, you will enter the RTR configuration mode.

IP SLAs allows a maximum of 2000 operations.

Debugging is supported only on the first 32 operation numbers.

After you configure a operation, you must schedule the operation. For information on scheduling a operation, refer to the **rtr schedule** and **rtr group schedule**global configuration commands. You can also optionally set reaction triggers for the operation. For information on reaction triggers, refer to the **rtr reaction-configuration** and **rtr reaction-trigger** global configuration commands.

Note After you schedule an operation, you cannot modify the configuration of the operation. To modify the configuration of the operation after it is scheduled, you must first delete the IP SLAs operation (using the **no rtr** command) and then reconfigure the operation with the new operation parameters.

To display the current configuration settings of the operation, use the **show rtr configuration**EXEC command.

Examples

In the following example, operation 1 is configured to perform end-to-end IP SLAs operations using an SNA LU Type 0 connection with the host name cwbc0a. Only the **type** RTR configuration command is required; all others are optional.

```
rtr 1
 type echo protocol snalu0echoappl cwbc0a
 request-data-size 40
 response-data-size 1440
```

Note If operation 1 already existed and it has not been scheduled, you are placed into RTR configuration mode. If the operation already exists and has been scheduled, this command will fail.

Related Commands

Command	Description
rtr group schedule	Configures the group scheduling parameters for multiple IP SLAs operations.
rtr reaction-configuration	Configures certain actions to occur based on events under the control of IP SLAs.
rtr reaction-trigger	Defines a second IP SLAs operation to make the transition from a pending state to an active state when one of the trigger action type options are defined with the ip sla monitor reaction-configuration command.
rtr schedule	Configures the scheduling parameters for a single IP SLAs operation.
show rtr configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

rtr group schedule

Note Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr group schedule**command is replaced by the **ip sla monitor group schedule** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr group schedule**command is replaced by the **ip sla group schedule** command. See the **ip sla monitor group schedule** and **ip sla group schedule** commands for more information.

To perform group scheduling for Cisco IOS IP Service Level Agreements (IP SLAs) operations, use the **rtr group schedule** command in global configuration mode. To stop the operation and place it in the default state of normal scheduling, use the **no** form of this command.

rtr group schedule *group-operation-number operation-id-numbers* **schedule-period** *schedule-period-range* [**ageout** *seconds*] [**frequency** *group-operation-frequency*] [**life** {**forever**| *seconds*}] [**start-time** {*hh* : *mm* [: *ss*] [*month day*| *day month*]| **pending**| **now**| **after** *hh* : *mm* : *ss*}]

no rtr group schedule

Syntax Description

group-operation-number	Group configuration or group schedule number of the IP SLAs operation to be scheduled. The range is from from 0 to 65535.
operation-id-numbers	The list of IP SLAs operation ID numbers in the scheduled operation group. Indicate ranges of operation ID numbers with a hyphen. Individual ID numbers and ranges of ID numbers are delimited by a comma. For example, enter a list of operation ID numbers in any of the following ways: • 2, 3, 4, 9, 20 • 10-20, 30-35, 60-70 • 2, 3, 4, 90-100, 105-115 The *operation-id-numbers* argument can include a maximum of 125 characters.
schedule-period *schedule-period-range*	Time (in seconds) for which the IP SLAs operation group is scheduled. The range is from 1 to 604800.
ageout *seconds*	(Optional) Number of seconds to keep the operation in memory when it is not actively collecting information. The default is 0 (never ages out).

frequency *group-operation-frequency*	(Optional) Specifies the number of seconds after which each IP SLAs operation is restarted. If this keyword and argument are specified, the frequency of all operations belonging to the group will be overridden and set to the specified frequency. The range is from 1 to 604800. **Note** If this keyword and argument are not specified, the frequency for each operation is set to the value specified for the schedule period.
life forever	(Optional) Schedules the operation to run indefinitely.
life *seconds*	(Optional) Number of seconds the operation actively collects information. The default is 3600 (one hour).
start-time	(Optional) Time when the operation starts collecting information. If the **start-time** is not specified, no information is collected until the **start-time** is configured or a trigger occurs that performs a **start-time now**.
hh **:** *mm* [**:** *ss*]	(Optional) Specifies an absolute start time using hours, minutes, and (optionally) seconds. Use the 24-hour clock notation. For example, **start-time 01:02** means "start at 1:02 a.m.," and **start-time 13:01:30** means "start at 1:01 p.m. and 30 seconds." The current day is implied unless you specify a *month* and *day*.
month	(Optional) Name of the month to start the operation in. If month is not specified, the current month is used. Use of this argument requires that a day be specified as well. You can specify the month by using either the full English name or the first three letters of the month.
day	(Optional) Number of the day (in the range 1 to 31) to start the operation on. If a day is not specified, the current day is used. Use of this argument requires that a month be specified as well.
pending	(Optional) No information is collected. This is the default value.
now	(Optional) Indicates that the operation should start immediately.

after *hh* **:** *mm* **:** *ss*	(Optional) Indicates that the operation should start *hh* hours, *mm* minutes, and *ss* seconds after this command was entered.

Command Default

The operation is placed in a **pending** state (that is, the operation is enabled but is not actively collecting information).

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(14)T	This command was replaced by the **ip sla monitor group schedule**command.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was replaced by the **ip sla monitor group schedule**command.
12.2(33)SRB	This command was replaced by the **ip sla group schedule**command.

Usage Guidelines

Though IP SLAs multiple operations scheduling functionality helps in scheduling thousands of operations, you should be cautious while specifying the number of operations, the schedule period, and the operation group frequency to avoid CPU hogging.

For example, consider a scenario where you are scheduling 1 to 780 operations at a schedule period of 60 seconds, the command would be as follows:

rtr group schedule 2 1-780 schedule-period 60 start-now

IP SLAs calculates how many operations it should start in each 1-second interval by dividing the number of operations by the schedule period (780 operations divided by 60 seconds, which is 13 operations per second). Operations 1 to 13 in operation group 2 start after 0 seconds, operations 14 to 26 start after 1 second, operations 27 to 40 start after 2 seconds, and the iteration continues until operations 768 to 780 start after 59 seconds. This high value of operations starting at every 1-second interval (especially for jitter operations) can load the CPU to very high values.

The maximum recommended value of operations per second is 6 or 7. This is approximately 350 to 400 operations per minute. This value of 6 or 7 operation per second will be the maximum that does not have any

major performance (CPU) impact. However, this value varies from platform to platform. The above value is verified and tested on a Cisco 2600 router.

Note No warning messages will be displayed if IP SLAs multiple operations scheduling leads to a high number of operations starting per second.

When you reboot the router, the IP SLAs multiple operations scheduling functionality schedules the operations in the same order as was done before the reboot. For example, assume the following operation had been scheduled:

rtr group schedule 2 1-20 schedule-period 40 start-time now

Over a range of 40 seconds, 20 operations have to be started (that is, one operation every 2 seconds). After the system reboot, operation 1 will start at *t* seconds and operation 2 starts at *t* +2 seconds, operation 3 starts at *t* +4 seconds, and so on.

The IP SLAs multiple operations scheduling functionality schedules the maximum number of operations possible without aborting. However, this functionality skips those IP SLAs operations that are already running or those that are not configured and hence do not exist. The total number of operations will be calculated based on the number of operations specified in the command, irrespective of the number of operations that are missing or already running. The IP SLAs multiple operations scheduling functionality displays a message showing the number of active and missing operations. However, these messages are displayed only if you schedule operations that are not configured or are already running.

Examples

The following example shows how to schedule IP SLAs operations 3, 4, and 6 to 10 in operation group 1:

```
rtr group schedule 1 3, 4, 6-10
```

The following example shows how to schedule IP SLAs operations 3, 4, and 6 to 10 in operation group 1, with a schedule period of 20 seconds:

```
rtr group schedule 1 3, 4, 6-10 schedule-period 20
```

The following example shows how to schedule IP SLAs operations 3, 4, and 6 to 10 in operation group 1, with a schedule period of 20 seconds with start time as now:

```
rtr group schedule 1 3, 4, 6-10 schedule-period 20 start-time now
```

Related Commands

Command	Description
rtr schedule	Enters rtr scheduling mode.
show rtr collection-statistics	Displays the collection details of the IP SLAs operation.
show rtr configuration	Displays the configuration details of the IP SLAs operation.
show rtr operation	Displays the operation details of the IP SLAs operation.

rtr key-chain

Note Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr key-chain**command is replaced by the **ip sla monitor key-chain** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr key-chain**command is replaced by the **ip sla key-chain** command. See the **ip sla monitor key-chain** and **ip sla key-chain** commands for more information.

To enable Cisco IOS IP Service Level Agreements (IP SLAs) control message authentication and specify an MD5 key chain, use the **rtr key-chain** command in global configuration mode. To remove control message authentication, use the no form of this command.

rtr key-chain *name*

no rtr key-chain

Syntax Description

name	Name of MD5 key chain.

Command Default

Control message authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.3(14)T	This command was replaced by the **ip sla monitor key-chain**command.
12.2(31)SB2	This command was replaced by the **ip sla monitor key-chain** command.
12.2(33)SRB	This command was replaced by the **ip sla key-chain**command.

Usage Guidelines

The authentication configuration on the IP SLAs source and IP SLAs Responder devices must be the same. In other words, both devices must be configured with the same key chain or both devices must not use authentication.

If the **rtr key-chain** command is entered, at least one key must be added to the specified MD5 key chain in order for MD5 authentication to occur.

Examples

In the following example, the IP SLAs control message uses MD5 authentication, and the key chain name is CSAA. The authentication string for key 1 is csaakey1.

```
rtr key-chain csaa
key chain csaa
key 1
key-string csaakey1
```

Related Commands

Command	Description
key	Identifies an authentication key on a key chain.
key chain	Enables authentication for routing protocols and identifies a group of authentication keys.
key-string (authentication)	Specifies the authentication string for a key.
rtr	Specifies an IP SLAs operation and enters RTR configuration mode.

rtr logging traps

Note Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr logging traps**command is replaced by the **ip sla monitor logging traps** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr logging traps**command is replaced by the **ip sla logging traps** command. See the **ip sla monitor logging traps** and **ip sla logging traps** commands for more information.

To enable the generation of Simple Network Management Protocol (SNMP) system logging messages specific to Cisco IOS IP Service Level Agreements (SLAs) trap notifications, use the **rtr logging traps** command in global configuration mode. To disable IP SLAs system logging SNMP traps, use the **no** form of this command.

rtr logging traps

no rtr logging traps

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP system logging messages specific to IP SLAs trap notifications are not generated.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(14)T	This command was replaced by the **ip sla monitor logging traps**command.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was replaced by the **ip sla monitor logging traps** command.
12.2(33)SRB	This command was replaced by the **ip sla logging traps** command.

Usage Guidelines

SNMP trap notifications 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 five 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 threshold violations. To configure proactive threshold monitoring parameters for an IP SLAs operation, use the **rtr reaction-configuration**command in global configuration mode.

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

Examples

The following example shows the configuration of IP SLAs traps to be triggered for round-trip time (RTT) violations and Voice over IP (VoIP) mean opinion score (MOS) violations, and the necessary SNMP configuration for enabling these SNMP logging traps:

```
rtr 1
 type jitter dest-ipaddr 209.165.200.225 dest-port 9234
!
rtr schedule 1 start now life forever
rtr reaction-configuration 1 react rtt threshold-type immediate threshold-value 3000 2000
action-type trapOnly
rtr reaction-configuration 1 react MOS threshold-type consecutive 4 threshold-value 390 220
 action-type trapOnly
!
rtr logging traps
snmp-server enable traps rtr
```

Related Commands

Command	Description
logging on	Controls (enables or disables) system message logging globally.
rtr reaction-configuration	Configures proactive threshold monitoring parameters for an IP SLAs operation.

rtr low-memory

Note Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr low-memory**command is replaced by the **ip sla monitor low-memory** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr low-memory**command is replaced by the **ip sla low-memory** command. See the **ip sla monitor low-memory** and **ip sla low-memory** commands for more information.

To specify how much unused memory must be available to allow Cisco IOS IP Service Level Agreements (IP SLAs) configuration, use the **rtr low-memory**command in global configuration mode. To remove the type configuration for the operation, use the **no** form of this command.

rtr low-memory *value*

no rtr low-memory

Syntax Description

value	Specifies amount of memory, in bytes, that must be available to configure IP SLAs. The range is from 0 to the maximum amount of free memory bytes available.

Command Default

The default *value* is 25 percent of the memory available on the system.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(14)T	This command was replaced by the **ip sla monitor low-memory**command.
12.2(31)SB2	This command was replaced by the **ip sla monitor low-memory** command.
12.2(33)SRB	This command was replaced by the **ip sla low-memory** command.

Usage Guidelines

The **rtr low-memory** command allows the user to specify the amount of memory that IP SLAs can use. If the amount of available free memory falls below the value specified in the **rtr low-memory** command, then you will not be allowed to configure new IP SLAs operations. If this command is not used, the default

low-memory value is 25 percent. This means that if 75 percent of system memory has been utilized you will not be able to configure any IP SLAs characteristics.

The value of the **rtr low-memory** command should not exceed the amount of free memory available on the system. To determine the amount of free memory available on the system, use the **show memory** EXEC command.

Examples

In the following example, the router is configured so that no less than 2 MB of memory will be free for IP SLAs configuration:

```
rtr low-memory 2000000
```

Related Commands

Command	Description
rtr	Specifies an identification number for an IP SLAs operation and enters RTR configuration mode.
show memory	Displays statistics about memory, including memory-free pool statistics.

rtr mpls-lsp-monitor

Note Effective with Cisco IOS Releases 12.2(31)SB2 and 12.2(33)SRB, the **rtr mpls-lsp-monitor**command is replaced by the **auto ip sla mpls-lsp-monitor**command. See the **auto ip sla mpls-lsp-monitor**command for more information.

To begin configuration for an IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation and enter SAA Multiprotocol Label Switching (MPLS) configuration mode, use the **rtr mpls-lsp-monitor** command in global configuration mode. To remove all configuration information for an LSP Health Monitor operation, use the **no** form of this command.

rtr mpls-lsp-monitor *operation-number*

no rtr mpls-lsp-monitor *operation-number*

Syntax Description

operation-number	Number used for the identification of the LSP Health Monitor operation you wish to configure.

Command Default

No LSP Health Monitor operation is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was replaced by the **auto ip sla mpls-lsp-monitor**command.
12.2(33)SRB	This command was replaced by the **auto ip sla mpls-lsp-monitor**command.

Usage Guidelines

Entering this command automatically enables the **mpls discovery vpn next-hop** command.

After you configure an LSP Health Monitor operation, you must schedule the operation. To schedule an LSP Health Monitor operation, use the **rtr mpls-lsp-monitor schedule** command in global configuration mode. You can also optionally set reaction configuration for the operation (see the **rtr mpls-lsp-monitor reaction-configuration** command).

To display the current configuration settings of an LSP Health Monitor operation, use the **show rtr mpls-lsp-monitor configuration** command in EXEC mode.

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router.

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
rtr mpls-lsp-monitor 1
 type echo saa-vrf-all
 timeout 1000
 scan-interval 1
 secondary-frequency connection-loss 10
 secondary-frequency timeout 10
!
rtr mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type consecutive
 3 action-type trapOnly
rtr mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3
action-type trapOnly
rtr logging traps
!
rtr mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
rtr mpls-lsp-monitor reaction-configuration	Configures certain actions to occur based on events under the control of the IP SLAs LSP Health Monitor.
rtr mpls-lsp-monitor schedule	Configures the scheduling parameters for an IP SLAs LSP Health Monitor operation.
show rtr mpls-lsp-monitor configuration	Displays configuration settings for IP SLAs LSP Health Monitor operations.
type echo (MPLS)	Configures the parameters for a Cisco IOS IP SLAs LSP ping operation using the LSP Health Monitor.
type pathEcho (MPLS)	Configures the parameters for a Cisco IOS IP SLAs LSP traceroute operation using the LSP Health Monitor.

rtr mpls-lsp-monitor reaction-configuration

Note Effective with Cisco IOS Releases 12.2(31)SB2 and 12.2(33)SRB, the **rtr mpls-lsp-monitor reaction-configuration**command is replaced by the **auto ip sla mpls-lsp-monitor reaction-configuration** command. See the **auto ip sla mpls-lsp-monitor reaction-configuration** command for more information.

To configure proactive threshold monitoring parameters for a Cisco IOS IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation, use the **rtr mpls-lsp-monitor reaction-configuration** command in global configuration mode. To clear all threshold monitoring configuration for a specified LSP Health Monitor operation, use the **no** form of this command.

rtr mpls-lsp-monitor reaction-configuration *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** {**consecutive** [*occurrences*]| **immediate**| **never**}]

no rtr mpls-lsp-monitor reaction-configuration *operation-number*

Syntax Description

operation-number	Number of the LSP Health Monitor operation for which reactions are to be configured.
react *monitored-element*	Specifies the element to be monitored for violations. Keyword options for the monitored element are: • **connectionLoss** --Specifies that a reaction should occur if there is a one-way connection loss for the monitored operation. • **timeout** --Specifies that a reaction should occur if there is a one-way timeout for the monitored operation.
action-type *option*	(Optional) Specifies what action or combination of actions the operation performs when threshold events occur. If the **threshold-type never** keywords are defined, the **action-type** keyword is disabled. The *option* argument can be one of the following keywords: • **none** --No action is taken. This option is the default value. • **trapOnly** --Send an SNMP logging trap when the specified violation type occurs for the monitored element.

threshold-type consecutive [*occurrences*]	(Optional) When a threshold violation for the monitored element is met consecutively for a specified number of times, perform the action defined by the **action-type** keyword. The default number of 5 consecutive occurrences can be changed using the *occurrences* argument. The range is from 1 to 16.
threshold-type immediate	(Optional) When a threshold violation for the monitored element is met, immediately perform the action defined by the **action-type** keyword.
threshold-type never	(Optional) Do not calculate threshold violations. This option is the default threshold type.

Command Default

IP SLAs proactive threshold monitoring is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was replaced by the **auto ip sla mpls-lsp-monitor reaction-configuration**command.
12.2(33)SRB	This command was replaced by the **auto ip sla mpls-lsp-monitor reaction-configuration** command.

Usage Guidelines

You can configure the **rtr mpls-lsp-monitor reaction-configuration** command multiple times to enable proactive threshold monitoring for multiple elements for the same operation. However, disabling of individual monitored elements is not supported. In other words, the **no rtr mpls-lsp-monitor reaction-configuration** command will disable all proactive threshold monitoring configuration for the specified IP SLAs operation.

SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB. Use the **rtr 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.

To display the current threshold monitoring configuration settings for an LSP Health Monitor operation, use the **show rtr mpls-lsp-monitor configuration** command.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router. As specified by the reaction condition configuration, when three consecutive connection loss or timeout events occur, an SNMP logging trap is sent.

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
rtr mpls-lsp-monitor 1
 type echo saa-vrf-all
 timeout 1000
 scan-interval 1
 secondary-frequency connection-loss 10
 secondary-frequency timeout 10
!
rtr mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type consecutive
 3 action-type trapOnly
rtr mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3
action-type trapOnly
rtr logging traps
!
rtr mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
rtr mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters SAA MPLS configuration mode.
show rtr mpls-lsp-monitor configuration	Displays configuration settings for IP SLAs LSP Health Monitor operations.

rtr mpls-lsp-monitor schedule

Note Effective with Cisco IOS Releases 12.2(31)SB2 and 12.2(33)SRB, the **rtr mpls-lsp-monitor schedule**command is replaced by the **auto ip sla mpls-lsp-monitor schedule** command. See the **auto ip sla mpls-lsp-monitor schedule** command for more information.

To configure the scheduling parameters for an IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor operation, use the **rtr mpls-lsp-monitor schedule** command in global configuration mode. To stop the operation and place it in the default state (pending), use the **no** form of this command.

rtr mpls-lsp-monitor schedule *operation-number* **schedule-period** *seconds* [**frequency** [*seconds*]] [**start-time** {**after** *hh* : *mm* : *ss*| *hh* : *mm* [: *ss*] [*month day*| *day month*]| **now**| **pending**}]

no rtr mpls-lsp-monitor schedule *operation-number*

Syntax Description

operation-number	Number of the LSP Health Monitor operation to be scheduled.
schedule-period *seconds*	Amount of time (in seconds) for which the LSP Health Monitor operation is scheduled.
frequency *seconds*	(Optional) Number of seconds after which each IP SLAs operation is restarted. The frequency is equal to the schedule period by default.
start-time	(Optional) Time when the operation starts collecting information. If the start time is not specified, no information is collected.
after *hh* **:** *mm* **:** *ss*	(Optional) Indicates that the operation should start *hh* hours, *mm* minutes, and *ss* seconds after this command was entered.
hh **:** *mm* [**:** *ss*]	(Optional) Specifies an absolute start time using hours, minutes, and seconds. Use the 24-hour clock notation. For example, **start-time 01:02** means “start at 1:02 a.m.,” and **start-time 13:01:30** means “start at 1:01 p.m. and 30 seconds.” The current day is implied unless you specify a month and day.
month	(Optional) Name of the month in which to start the operation. If a month is not specified, the current month is used. Use of this argument requires that a day be specified. You can specify the month by using either the full English name or the first three letters of the month.

day	(Optional) Number of the day (in the range 1 to 31) on which to start the operation. If a day is not specified, the current day is used. Use of this argument requires that a month be specified.
now	(Optional) Indicates that the operation should start immediately.
pending	(Optional) No information is collected. This option is the default value.

Command Default

The LSP Health Monitor operation is placed in a pending state (that is, the operation is enabled but is not actively collecting information).

Command Modes

Global configuration

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was replaced by the **auto ip sla mpls-lsp-monitor schedule**command.
12.2(33)SRB	This command was replaced by the **auto ip sla mpls-lsp-monitor schedule** command.

Usage Guidelines

After you schedule an LSP Health Monitor operation with the **rtr mpls-lsp-monitor schedule** command, you cannot change the configuration of the operation. To change the configuration of the operation, use the **no rtr mpls-lsp-monitor** *operation-number* command in global configuration mode and then enter the new configuration information.

To display the current configuration settings of an LSP Health Monitor operation, use the **show rtr mpls-lsp-monitor configuration** command in EXEC mode.

Examples

The following example shows how to configure operation parameters, reaction conditions, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all BGP next hop neighbors in use by all VRFs associated with the source Provider Edge (PE) router. As specified in the example configuration, the schedule period for LSP Health Monitor operation 1 is 60 seconds and the operation is scheduled to start immediately.

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
```

```
!
rtr mpls-lsp-monitor 1
 type echo saa-vrf-all
 timeout 1000
 scan-interval 1
 secondary-frequency connection-loss 10
 secondary-frequency timeout 10
!
rtr mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type consecutive
 3 action-type trapOnly
rtr mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive 3
action-type trapOnly
rtr logging traps
!
rtr mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
rtr mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters SAA MPLS configuration mode.
show rtr mpls-lsp-monitor configuration	Displays configuration settings for IP SLAs LSP Health Monitor operations.

rtr reaction-configuration

Note Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr reaction-configuration**command is replaced by the **ip sla monitor reaction-configuration** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr reaction-configuration**command is replaced by the **ip sla reaction-configuration** command. See the **ip sla monitor reaction-configuration** and **ip sla reaction-configuration** commands for more information.

To configure proactive threshold monitoring parameters for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **rtr reaction-configuration**command in global configuration mode. To clear all threshold monitoring configuration for a specified IP SLAs operation, use the **no** form of this command.

rtr reaction-configuration *operation-number* [**react** *monitored-element*] [**threshold-type** {**never**| **immediate**| **consecutive** [*consecutive-occurrences*]| **xofy** [*x-value y-value*]| **average** [*number-of-measurements*]}] [**threshold-value** *upper-threshold lower-threshold*] [**action-type** {**none**| **trapOnly**| **triggerOnly**| **trapAndTrigger**}]

no rtr reaction-configuration *operation-number*

Syntax Description

operation-number	Number of the IP SLAs operation to configure for which reactions are to be configured.
react *monitored-element*	Specifies the element to be monitored for threshold violations. Keyword options for the *monitored-element* are: **connectionLoss** --Specifies that a reaction should occur if there is a connection loss for the monitored operation. Thresholds do not apply to this monitored element. **jitterAvg** --Specifies that a reaction should occur if the average round-trip jitter value violates the upper threshold or lower threshold. **jitterDSAvg** --Specifies that a reaction should occur if the average destination-to-source (DS) jitter value violates the upper threshold or lower threshold. **jitterSDAvg** --Specifies that a reaction should occur if the average source-to-destination (SD) jitter value violates the upper threshold or lower threshold. **mos** --Specifies that a reaction should occur if the mean opinion score (MOS) value violates the upper threshold or lower threshold.

react *monitored-element* (continued)	**PacketLossDS** --Specifies that a reaction should occur if the destination-to-source packet loss value violates the upper threshold or lower threshold. **PacketLossSD** --Specifies that a reaction should occur if the source-to-destination packet loss value violates the upper threshold or lower threshold. **rtt** --Specifies that a reaction should occur if the mean opinion score (MOS) value violates the upper threshold or lower threshold. **timeout** --Specifies that a reaction should occur if there is a timeout for the monitored operation. Thresholds do not apply to this monitored element. **verifyError** --Specifies that a reaction should occur if there is an error verification violation. Thresholds do not apply to this monitored element.
threshold-type never	Do not calculate threshold violations. This is the default threshold-type.
threshold-type immediate	When a threshold violation is met for the monitored element, immediately perform the action defined by **action-type**.
threshold-type consecutive [*consecutive-occurences*]	When a threshold violation is met for the monitored element five times in a row, perform the action defined by **action-type**. The optional *consecutive-occurences* argument can be used to change the number of consecutive occurences from the default of 5. The valid range is from 1 to 16. The *consecutive-occurences* value will appear in the output of the **show rtr reaction-configuration** command as the “Threshold Count:” value.
threshold-type xofy [*x-value y-value*]	When a threshold violation is met for the monitored element after some number (x) of violations within some other number (y) of measurements (“x of y”), perform the action defined by action-type. The default is 5 for both *x-value* and *y-value* (**xofy 5 5**). The valid range for each value is from 1 to 16. The *x-value* value will appear in the output of the **show rtr reaction-configuration** command as the “Threshold Count:” value, and the *y-value* will appear as the “Threshold Count2:” value.

threshold-type average [*number-of-measurements*]	When the average of the last five values for the monitored element exceeds the upper threshold or when the average of the last five values for the monitored element drops below the lower threshold, perform the action defined by **action-type**. For example, if the upper threshold for **react rtt threshold-type average 3** is configured as 5000 ms and the last three results of the operation are 6000, 6000, and 5000 ms, the average would be 6000 + 6000 + 5000=17000/3 = 5667, thus violating the 5000-ms upper threshold. The default number of 5 averaged measurements can be changed using the optional *number-of-measurements* argument. The valid range from 1 to 16. This syntax is not available if **connectionLoss**, **timeout**, or **verifyError** is specified as the monitored element, as upper and lower thresholds do not apply to these options.
[**threshold-value** *upper-threshold lower-threshold*]	(Optional) Specifies the upper-threshold value and lower-threshold values, for **jitterAvg**, **jitterDSAvg**, **jitterSDAvg**, **mos**, **PacketLossDS**, **PacketLossSD**, and **rtt**. The default upper-threshold value for all monitored elements except mos is 4500, and the default lower-threshold value is 3000. For MOS threshold values (**react mos**), the number is expressed in 3 digits representing ones, tenths, and hundredths. For example, to express a MOS threshold of 3.20, enter **320**. The valid range is from 100 (1.00) to 500 (5.00). The default upper-threshold for MOS is 300 (3.00) and the default lower-threshold is 200 (2.00).

action-type *option*	(Optional) Specify what action or combination of actions the operation performs when you configure **connection-loss-enable** or **timeout-enable**, or threshold events occur. For the **action-type** to occur for threshold events, the **threshold-type** must be defined to anything other than **never**. Option can be one of the following keywords: • **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 **rtr 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 **rtr 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. The following SNA NMVT action-type options appear in the command line help, but are no longer valid: **nmvtOnly**, **trapAndNmvt**, **nmvtAndTrigger**, **trapNmvtAndTrigger**. These SNA NMVT CLI options will be removed in an upcoming release.

Command Default IP SLAs proactive threshold monitoring is disabled.

Command Modes Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Release	Modification
12.1(1)T	The **verify-error-enable** optional keyword was added.
12.3(7)T	This command was enhanced to provide new monitored elements and reaction options. The old syntax of **rtr reaction-configuration** *operation-number* [**verify-error-enable**] [**connection-loss-enable**] [**timeout-enable**] [**threshold-falling** *milliseconds*] [**threshold-type** *option*] [**action-type** *option*] was replaced by the syntax shown above. **Note** Configuration of IP SLAs reactions using the old syntax remains available in release 12.3(7)T for backwards compatibility, but support for the old syntax will be removed in an upcoming release. • The functionality of the **connection-loss-enable** keyword was replaced by the **react connectionLoss** syntax. • The functionality of the **timeout-enable** keyword was replaced by the **react timeout** syntax. • The functionality of the **verify-error-enable** keyword was replaced by the **react verifyError** syntax. • The functionality of the threshold-falling milliseconds syntax (and the threshold RTR configuration command) was replaced by the **threshold-value** *upper-threshold lower-threshold* syntax.
12.3(14)T	This command was replaced by the **ip sla monitor reaction-configuration**command.
12.2(31)SB2	This command was replaced by the **ip sla monitor reaction-configuration** command.
12.2(33)SRB	This command was replaced by the **ip sla reaction-configuration**command.

Usage Guidelines

You can configure the **rtr reaction-configuration** command multiple times to enable proactive threshold monitoring for multiple elements (for example, configuring thresholds for destination-to-source packet loss and MOS) for the same operation. However, disabling of individual monitored elements is not supported. In other words, the **no rtr reaction-configuration** command will disable all proactive threshold monitoring configuration for the specified IP SLAs operation.

SNMP traps for IP SLAs are supported by the CISCO-RTTMON-MIB. Use the **rtr 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.

To display the current threshold monitoring configuration settings for an IP SLAs operation, use the **show rtr configuration** command.

Examples

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

```
rtr reaction-configuration 10 react mos threshold-type immediate threshold-value 490 250
action-type trapOnly
```

Related Commands

Command	Description
rtr	Begins configuration for an IP SLAs operation and enters RTR configuration mode.
rtr logging traps	Enables the generation of SNMP system logging messages specific to IP SLAs trap notifications.
rtr reaction-trigger	Defines a second IP SLAs operation to make the transition from a pending state to an active state when one of the trigger action-type options are defined with the **rtr reaction-configuration** global configuration command.
show rtr reaction-configuration	Displays the configured proactive threshold monitoring settings for all IP SLAs operations or a specified operation.
show rtr reaction-trigger	Displays the configured state of triggered IP SLAs operations.

rtr reaction-trigger

Note Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr reaction-trigger**command is replaced by the **ip sla monitor reaction-trigger** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr reaction-trigger**command is replaced by the **ip sla reaction-trigger** command. See the **ip sla monitor reaction-trigger** and **ip sla reaction-trigger** commands for more information.

To define a second Cisco IOS IP Service Level Agreements (IP SLAs) operation to make the transition from a pending state to an active state when one of the trigger action-type options are defined with the **rtr reaction-configuration** command, use the **rtr reaction-trigger** command in global configuration mode. To remove the trigger combination, use the no form of this command.

rtr reaction-trigger *operation-number target-operation*

no rtr reaction-trigger *operation*

Syntax Description

operation-number	Number of the operation in the active state that has the **action-type** set with the **rtr reaction-configuration** globalconfiguration command.
target-operation	Number of the operation in the pending state that is waiting to be triggered with the **rtr**globalconfiguration command.

Command Default

No trigger combination is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(14)T	This command was replaced by the **ip sla monitor reaction-trigger**command.
12.2(31)SB2	This command was replaced by the **ip sla monitor reaction-trigger** command.
12.2(33)SRB	This command was replaced by the **ip sla reaction-trigger**command.

Usage Guidelines

Triggers are usually used for diagnostics purposes and are not used in normal operation.

Examples

In the following example, the state of operation 1 is changed from pending state to active state when **action-type of**operation 2 occurs:

```
rtr reaction-trigger 2 1
```

Related Commands

Command	Description
rtr	Specifies an IP SLAs operation and enters RTR configuration mode.
rtr reaction-configuration	Configures certain actions to occur based on events under the control of IP SLAs.
rtr schedule	Configures the scheduling parameters for an IP SLAs operation.

rtr reset

Note Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr reset**command is replaced by the **ip sla monitor reset** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr reset**command is replaced by the **ip sla reset** command. See the **ip sla monitor reset** and **ip sla reset** commands for more information.

To perform a shutdown and restart of the Cisco IOS IP Service Level Agreements (SLAs) engine, use the **rtr reset**command in global configuration mode.

rtr reset

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(14)T	This command was replaced by the **ip sla monitor reset**command.
12.2(31)SB2	This command was replaced by the **ip sla monitor reset** command.
12.2(33)SRB	This command was replaced by the **ip sla reset**command.

Usage Guidelines

The **rtr reset** command stops all operations, clears IP SLAs configuration information, and returns the IP SLAs feature to the startup condition. This command does not reread the IP SLAs configuration stored in startup-config in NVRAM. You must retype the configuration or load a previously saved configuration file.

Note The **rtr reset** command does not remove IP SLAs label switched path (LSP) Health Monitor configurations from the running configuration.

Caution Use the **rtr reset** command only in extreme situations such as the incorrect configuration of a number of operations.

Examples

The following example resets IP SLAs, clearing all stored IP SLAs information and configuration:

```
rtr reset
```

Related Commands

Command	Description
rtr restart	Restarts a stopped IP SLAs operation.

rtr responder

Note Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr responder**command is replaced by the **ip sla monitor responder** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr responder**command is replaced by the **ip sla responder** command. See the **ip sla monitor responder** and **ip sla responder** commands for more information.

To enable the Cisco IOS IP Service Level Agreements (IP SLAs) Responder on a destination (operational target) device, use the **rtr responder** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

rtr responder

no rtr responder

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.3(14)T	This command was replaced by the **ip sla monitor responder** command.
12.2(31)SB2	This command was replaced by the **ip sla monitor responder**command.
12.2(33)SRB	This command was replaced by the **ip sla responder**command.

Usage Guidelines

This command is used on the destination device for IP SLAs operations to enable the sending of receiving of IP SLAs Control packets. Enabling the IP SLAs Responder allows the generation of monitoring statistics on the device sending IP SLAs operations.

Examples

The following example enables the IP SLAs Responder:

```
rtr responder
```

Related Commands

Command	Description
rtr responder type tcpConnect	Enables the IP SLAs Responder for TCP Connect operations.
rtr responder type udpEcho	Enables the IP SLAs Responder for UDP Echo and Jitter operations.

rtr responder type tcpConnect

Note Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr responder type tcpConnect** command is replaced by the **ip sla monitor responder type tcpConnect ipaddress** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr responder type tcpConnect** command is replaced by the **ip sla responder tcp-connect ipaddress** command. See the **ip sla monitor type tcpConnect ipaddress** and **ip sla responder tcp-connect ipaddress** commands for more information.

To enable the Cisco IOS IP Service Level Agreements (IP SLAs) Responder for TCP Connect operations, use the **rtr responder type tcpConnect**command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

rtr responder type tcpConnect ipaddress *ip-address* **port** *port*

no rtr responder type tcpConnect ipaddress *ip-address* **port** *port*

Syntax Description

ipaddress *ip-address*	(Optional) Specifies the IP address that the operation will be received at.
port *port*	(Optional) Specifies the port number that the operation will be received on.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1(1)T	The **ipaddr** and **port** keywords were added.
12.3(14)T	This command was replaced by the **ip sla monitor responder type tcpConnect ipaddress**command.
12.2(31)SB2	This command was replaced by the **ip sla monitor responder type tcpConnect ipaddress** command.
12.2(33)SRB	This command was replaced by the **ip sla responder tcp-connect ipaddress**command.

Usage Guidelines

This command is used on the destination device for IP SLAs operations to enable the acceptance and return of TCP Connect operation packets.

Examples

The following example shows how to enable the IP SLAs Responder for TCP connection operations:

```
rtr responder type tcpConnect ipaddress A.B.C.D port 1
```

Related Commands

Command	Description
rtr	Specifies an IP SLAs operation and enters RTR configuration mode.
rtr responder type frame-relay	Enables the IP SLAs Responder for Frame Relay operations.
rtr responder type udpEcho	Enables the IP SLAs Responder for UDP Echo and Jitter operations.

rtr responder type udpEcho

Note Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr responder type udpEcho** command is replaced by the **ip sla monitor responder type udpEcho ipaddress** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr responder type udpEcho** command is replaced by the **ip sla responder udp-echo ipaddress** command. See the **ip sla monitor type udpEcho ipaddress** and **ip sla responder udp-echo ipaddress** commands for more information.

To enable the Cisco IOS IP Service Level Agreements (IP SLAs) Responder for User Datagram Protocol (UDP) Echo or Jitter operations, use the **rtr responder** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

rtr responder type udpEcho ipaddress *ip-address* **port** *port*

no rtr responder type udpEcho ipaddress *ip-address* **port** *port*

Syntax Description

ipaddress *ip-address*	Specifies the IP address that the operation will be received at.
port *port*	Specifies the port number that the operation will be received on.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.3(14)T	This command was replaced by the **ip sla monitor responder type udpEcho ipaddress**command.
12.2(31)SB2	This command was replaced by the **ip sla monitor responder type udpEcho ipaddress** command.
12.2(33)SRB	This command was replaced by the **ip sla responder udp-echo ipaddress**command.

Usage Guidelines

This command is used on the destination device for IP SLAs operations to enable UPD Echo and Jitter (UDP+) operations on non-native interfaces.

Examples

The following example enables the IP SLAs Responder for Jitter operations:

```
rtr responder type udpEcho ipaddress A.B.C.D port 1
```

Related Commands

Command	Description
rtr responder	Enables the IP SLAs Responder for non-specific IP SLAs operations.
rtr responder type frame-relay	Enables the IP SLAs Responder for Frame Relay operations.

rtr restart

Note Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr restart**command is replaced by the **ip sla monitor restart** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr restart**command is replaced by the **ip sla restart** command. See the **ip sla monitor restart** and **ip sla restart** commands for more information.

To restart a Cisco IOS IP Service Level Agreements (IP SLAs) operation, use the **rtr restart** command in global configuration mode.

rtr restart *operation-number*

Syntax Description

operation-number	Number of the IP SLAs operation to restart. IP SLAs allows a maximum of 2000 operations.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	The maximum number of operations was increased from 500 to 2000 (SAA Engine II).
12.3(14)T	This command was replaced by the **ip sla monitor restart**command.
12.2(31)SB2	This command was replaced by the **ip sla monitor restart**command.
12.2(33)SRB	This command was replaced by the **ip sla restart**command.

Usage Guidelines

To restart an operation, the operation should be in an “active” state (as defined in the **rtr reaction-configuration** command).

IP SLAs allows a maximum of 2000 operations.

This command does not have a **no** form.

Examples

The following example restarts operation 12:

```
rtr restart 12
```

Related Commands

Command	Description
rtr reset	Clears all current IP SLAs statistics and configuration information from the router and resets the IP SLAs engine.

rtr schedule

Note Effective with Cisco IOS Release 12.3(14)T and 12.2(31)SB2, the **rtr schedule**command is replaced by the **ip sla monitor schedule** command. Effective with Cisco IOS Release 12.2(33)SRB, the **rtr schedule**command is replaced by the **ip sla schedule** command. See the **ip sla monitor schedule** and **ip sla schedule** commands for more information.

To configure the scheduling parameters for a Cisco IOS IP Service Level Agreements (IP SLAs) single operation, use the **rtr schedule**command in global configuration mode. To stop the operation and place it in the default state (**pending**), use the **no** form of this command.

rtr schedule *group-operation-number* [**life** {**forever**| *seconds*}] [**start-time** {*hh* : *mm* [: *ss*] [*month day*| *day month*]| **pending**| **now**| **after** *hh* : *mm* : *ss*}] [**ageout** *seconds*] **[recurring]**

no rtr schedule *group-operation-number*

Syntax Description

group-operation-number	Group configuration or group schedule number of the IP SLAs operation to schedule.
life forever	(Optional) Schedules the operation to run indefinitely.
life *seconds*	(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour).
start-time	Time when the operation starts.
hh **:** *mm* [**:** *ss*]	Specifies an absolute start time using hour, minute, and (optionally) second. Use the 24-hour clock notation. For example, **start-time 01:02** means "start at 1:02 a.m.," and **start-time 13:01:30** means "start at 1:01 p.m. and 30 seconds." The current day is implied unless you specify a *month* and *day*.
month	(Optional) Name of the month to start the operation in. If month is not specified, the current month is used. Use of this argument requires that a day be specified as well. You can specify the month by using either the full English name or the first three letters of the month.
day	(Optional) Number of the day (in the range 1 to 31) to start the operation on. If a day is not specified, the current day is used. Use of this argument requires that a month be specified as well.

pending	(Optional) No information is collected. This is the default value.
now	(Optional) Indicates that the operation should start immediately.
after *hh* **:** *mm* **:** *ss*	(Optional) Indicates that the operation should start *hh* hours, *mm* minutes, and *ss* seconds after this command was entered.
ageout *seconds*	(Optional) Number of seconds to keep the operation in memory when it is not actively collecting information. The default is 0 seconds (never ages out).
recurring	(Optional) Indicates that the operation will start automatically at the specified time and for the specified duration every day.

Command Default

The operation is placed in a **pending** state (that is, the operation is enabled but not actively collecting information).

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	The **after** and **forever** keywords were added.
12.3(8)T	The **recurring** keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S. This integration includes the addition of the **recurring** keyword.
12.3(14)T	This command was replaced by the **ip sla monitor schedule**command.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC. This integration includes the addition of the **recurring** keyword.
12.2(31)SB2	This command was replaced by the **ip sla monitor schedule**command.
12.2(33)SRB	This command was replaced by the **ip sla restart**command.

Usage Guidelines

After you schedule the operation with the **rtr schedule** command, you cannot change the configuration of the operation. To change the configuration of the operation, use the **no** form of the **rtr**global configuration command and reenter the configuration information.

If the operation is in a pending state, you can define the conditions under which the operation makes the transition from pending to active with the **rtr reaction-trigger**and **rtr reaction-configuration** global configuration commands. When the operation is in an active state, it immediately begins collecting information.

The following time line shows the age-out process of the operation:

```
W---------------------X---------------------Y---------------------Z
```

where:

- W is the time the operation was configured with the **rtr** global configuration command.
- X is the start time or start of life of the operation (that is, when the operation became “active”).
- Y is the end of life as configured with the **rtr schedule** global configuration command (life seconds have counted down to zero).
- Z is the age out of the operation.

Age out starts counting down at W and Y, is suspended between X and Y, and is reset to its configured size at Y.

It is possible for the operation to age out before it executes (that is, Z can occur before X). To ensure that this does not happen, the difference between the operation’s configuration time and start time (X and W) must be less than the age-out seconds.

Note The total RAM required to hold the history and statistics tables is allocated at the time of scheduling the IP SLAs operation. This prevents router memory problems when the router gets heavily loaded and lowers the amount of overhead an IP SLAs operation causes on a router when it is active.

The **recurring** keyword is only supported for scheduling single IP SLAs operations. You cannot schedule multiple IP SLAs operations using the **rtr schedule** command. The **life** value for a recurring IP SLAs operation should be less than one day. The **ageout** value for a recurring operation must be “never” (which is specified with the value 0), or the sum of the **life** and **ageout**values must be more than one day. If the **recurring** option is not specified, the operations are started in the existing normal scheduling mode.

Examples

In the following example, operation 25 begins actively collecting data at 3:00 p.m. on April 5. This operation will age out after 12 hours of inactivity, which can be before it starts or after it has finished with its life. When this operation ages out, all configuration information for the operation is removed (that is, the configuration information is no longer in the running-config in RAM).

```
rtr schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

In the following example, operation 1 begins collecting data after a 5-minute delay:

```
rtr schedule 1 start after 00:05:00
```

In the following example, operation 3 begins collecting data immediately and is scheduled to run indefinitely:

```
rtr schedule 3 start-time now life forever
```

In the following example, operation 15 begins automatically collecting data every day at 1:30 a.m.:

```
rtr schedule 15 start-time 01:30:00 recurring
```

Related Commands

Command	Description
rtr	Specifies an IP SLAs operation and enters RTR configuration mode.
rtr group schedule	Performs group scheduling for IP SLAs operations.
rtr reaction-configuration	Configures certain actions to occur based on events under the control of IP SLAs.
rtr reaction-trigger	Defines a second IP SLAs operation to make the transition from a pending state to an active state when one of the trigger action-type options is defined with the **rtr reaction-configuration** global configuration command.
show rtr configuration	Displays the configuration details of the IP SLAs operation.

samples-of-history-kept

To set the number of entries kept in the history table per bucket for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **samples-of-history-kept**command in the appropriate submode of IP SLA configuration or IP SLA monitor configuration mode. To return to the default value, use the **no** form of this command.

samples-of-history-kept *samples*

no samples-of-history-kept

Syntax Description

samples	Number of entries kept in the history table per bucket. The default is 16.

Command Default

16 entries

Command Modes

ICMP path echo configuration (config-ip-sla-pathEcho)

Command Modes

ICMP path echo configuration (config-sla-monitor-pathEcho)

Note The configuration mode varies depending on the Cisco IOS release you are running and the operation type configured. See the "Usage Guidelines" section for more information.

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An IP SLAs operation can collect history and capture statistics. By default, the history for an IP SLAs operation is not collected. If history is collected, each history bucket contains one or more history entries from the operation. When the operation type is ICMP path echo, an entry is created for each hop along the path that the operation takes to reach its destination. The type of entry stored in the history table is controlled by the

filter-for-history command. The total number of entries stored in the history table is controlled by the combination of the **samples-of-history-kept**, **buckets-of-history-kept**, and **lives-of-history-kept** commands.

Note This command is supported by the IP SLAs ICMP path echo operation only.

Note Collecting history increases the RAM usage. Collect history only when you think there is a problem in the network.

IP SLAs Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see the table below). You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation.

The configuration mode for the **samples-of-history-kept** command varies depending on the Cisco IOS release you are running (see the table below) and the operation type configured. For example, if you are running Cisco IOS Release 12.4 and the ICMP path echo operation type is configured, you would enter the **samples-of-history-kept** command in ICMP path echo configuration mode (config-sla-monitor-pathEcho) within IP SLA monitor configuration mode.

Table 9: Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(4)T, 12.0(32)SY, 12.2(33)SRB, 12.2(33)SB, 12.2(33)SXI , or later releases	**ip sla**	IP SLA configuration
12.3(14)T, 12.4, 12.4(2)T, 12.2(31)SB2, or 12.2(33)SXH	**ip sla monitor**	IP SLA monitor configuration

Examples

In the following examples, ten entries are kept in the history table for each of the lives of IP SLAs ICMP path echo operation 1. Note that the Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see the table above).

Examples

```
ip sla 1
 path-Echo 172.16.1.176
 history lives-kept 3
 samples-of-history-kept 10
!
ip sla schedule 1 life forever start-time now
```

Examples

```
ip sla monitor 1
 type pathecho protocol ipIcmpEcho 172.16.1.176
 lives-of-history-kept 3
 samples-of-history-kept 10
```

```
!
ip sla monitor schedule 1 life forever start-time now
```

Related Commands

Command	Description
buckets-of-history-kept	Sets the number of history buckets that are kept during the lifetime of the IP SLAs operation.
filter-for-history	Defines the type of information kept in the history table for the IP SLAs operation.
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
lives-of-history-kept	Sets the number of lives maintained in the history table for the IP SLAs operation.

scan-interval

To specify the time interval at which the IP Service Level Agreements (SLAs) label switched path (LSP) Health Monitor checks the scan queue for Border Gateway Protocol (BGP) next hop neighbor updates, use the **scan-interval** command in auto IP SLA MPLS parameters configuration mode. To return to the default value, use the **no** form of this command.

scan-interval *minutes*

no scan-interval

Syntax Description

minutes	Specifies the time interval (in minutes) at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates.

Command Default

Scan interval is 240 minutes.

Command Modes

Auto IP SLA MPLS parameters configuration (config-auto-ip-sla-mpls-params)

Command History

Release	Modification
12.2(27)SBC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

At each scan interval, a new IP SLA operation is automatically created for each newly discovered BGP next hop neighbor listed in the LSP Health Monitor scan queue. If there is more than one IP SLAs operation created at a specific scan interval, the start time for each newly created IP SLAs operation is randomly distributed to avoid having all of the operations start at the same time.

Use the **delete-scan-factor** command in IP SLA monitor configuration mode to specify the number of times the LSP Health Monitor should check the scan queue before automatically deleting IP SLAs operations for BGP next hop neighbors that are no longer valid.

You must configure the type of LSP Health Monitor operation (such as LSP ping) before you can configure any of the other parameters of the operation.

Note The default interval of time that BGP neighbor statistics are updated is different for the IP SLAs LSP Health Monitor database and the BGP next hop neighbor discovery database. Use the **scan-interval** command to set the timer for the IP SLAs LSP Health Monitor database. Use the **mpls discovery vpn interval** command to set the timer for the BGP next hop neighbor discovery database.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing and forwarding (VRF) instances associated with the source Provider Edge (PE) router. The time interval at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates is set to 1 minute.

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 timeout 1000
 scan-interval 1
 secondary-frequency connection-loss 10
 secondary-frequency timeout 10
 delete-scan-factor 2
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive
 3 action-type trapOnly
ip sla logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
delete-scan-factor	Specifies the number of times the LSP Health Monitor should check the scan queue before automatically deleting IP SLAs operations for BGP next hop neighbors that are no longer valid.
show ip sla mpls-lsp-monitor scan-queue	Displays information about adding or deleting BGP next hop neighbors from a particular MPLS VPN of an IP SLAs LSP Health Monitor operation.

scan-period

To set the amount of time after which the label switched path (LSP) discovery process can restart for a Cisco IOS IP Service Level Agreements (SLAs) LSP Health Monitor operation, use the **scan-period** command in auto IP SLA MPLS LSP discovery parameters configuration mode. To return to the default value, use the **no** form of this command.

scan-period *minutes*

no scan-period

Syntax Description

minutes	The amount of time (in minutes) after which the LSP discovery process can restart. The default is 1.

Command Default

1 minute

Command Modes

Auto IP SLA MPLS LSP discovery parameters configuration (config-auto-ip-sla-mpls-lpd-params)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

When the LSP discovery process has completed one iteration of discovering the equal-cost multipaths for each applicable Border Gateway Protocol (BGP) next hop neighbors associated with a single LSP Health Monitor operation, the next iteration of the LSP discovery process will start immediately if the time period set by the **scan-period** command has expired. If this rediscovery time period has not yet expired, then the next iteration of the LSP discovery process will not start until the time period has expired.

Setting the LSP rediscovery time period to 0 will cause the LSP discovery process to always restart immediately after completing one iteration of discovering the equal-cost multipaths for each applicable BGP next hop neighbor associated with a single LSP Health Monitor operation.

Use the **path-discover** command to enable the LSP discovery option for an IP SLAs LSP Health Monitor operation and enter auto IP SLA MPLS LSP discovery parameters configuration mode.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, the LSP discovery option is enabled for LSP Health Monitor operation 1. Operation 1 is configured to automatically create IP SLAs LSP ping operations for the equal-cost multipaths to all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN

routing and forwarding (VRF) instances associated with the source Provider Edge (PE) router. The LSP rediscovery time period is set to 30 minutes.

```
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 path-discover
!
 maximum-sessions 2
 session-timeout 60
 interval 2
 timeout 4
 force-explicit-null
 hours-of-statistics-kept 1
 scan-period 30
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 frequency 100 start-time now
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd tree-trace action-type
trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group retry 3 action-type
 trapOnly
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS LSP discovery parameters configuration mode.

schedule

To add an auto IP Service Level Agreements (SLAs) scheduler to the configuration of an IP SLAs auto-measure group, use the **schedule** command in IP SLA auto-measure group configuration mode. To stop operations of the group, use the **no** form of this command.

schedule *schedule-id*

no schedule *schedule-id*

Syntax Description

schedule-id	ID of an already-configured auto IP SLAs scheduler.

Command Default

The operation in the group being configured is not scheduled.

Command Modes

IP SLA auto-measure group configuration (config-am-group)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command specifies an auto IP SLAs scheduler as a reference for the IP SLAs auto-measure group being configured.

Only one auto IP SLAs scheduler can be specified for each IP SLAs auto-measure group. Each scheduler can be referenced by more than one group.

To create a multioperation schedule, specify the same auto IP SLAs scheduler for two or more IP SLAs auto-measure groups.

You cannot modify the configuration of an auto-measure group if the specified auto IP SLAs scheduler has a start time other than Pending trigger (default). If you attempt to modify a group configuration that includes an active scheduler, the following message appears:

```
%Group is active, cannot make changes
```

To modify the configuration of an IP SLAs auto-measure group that includes an active auto IP SLAs scheduler with a specified start time, use the **no** form of this command to remove the scheduler from the group configuration, and then finish configuring the group before adding an active scheduler to the configuration. You can also configure the start time for a scheduler after adding the scheduler to the group configuration.

To create an auto IP SLAs scheduler, use the **ip sla auto schedule** command.

Examples

The following example shows how to add an auto IP SLAs scheduler to the configuration of an IP SLAs auto-measure group:

```
Router(config)#ip sla auto group type ip 1

Router(config-am-grp)#destination 1
Router(config-am-grp)#schedule 1
Router(config-am-grp)#end
Router#
Router# show ip sla auto group
Group Name: 1
    Description:
    Activation Trigger: Pending
    Destination: 1
    Schedule: 1
IP SLAs Auto Template: default
    Measure Type: icmp-jitter
    Description:
    IP options:
        Source IP: 0.0.0.0
        VRF:    TOS: 0x0
    Operation Parameters:
        Number of Packets: 10   Inter packet interval: 20
        Timeout: 5000           Threshold: 5000
    Statistics Aggregation option:
        Hours of statistics kept: 2
    Statistics Distributions options:
        Distributions characteristics: RTT
        Distributions bucket size: 20
        Max number of distributions buckets: 1
    Reaction Configuration: None
IP SLAs auto-generated operations of group 1
    no operation created
```

Related Commands

Command	Description
ip sla auto schedule	Begins configuration for an auto IP SLAs scheduler and enters IP SLA auto-measure schedule configuration mode.

secondary-frequency

To set a faster measurement frequency (secondary frequency) to which a Cisco IOS IP Service Level Agreements (SLAs) operation should change when a reaction condition occurs, use the **secondary-frequency** command in the appropriate submode of auto IP SLA MPLS configuration, IP SLA configuration, or IP SLA monitor configuration mode. To disable the secondary frequency, use the **no** form of this command.

secondary-frequency {**both| connection-loss| timeout**} *frequency*

no secondary-frequency {**connection-loss| timeout**}

Syntax Description

both	Specifies that the operation measurement frequency should increase to the secondary frequency value if a one-way connection loss or one-way timeout is detected.
connection-loss	Specifies that the operation measurement frequency should increase to the secondary frequency value if a one-way connection loss is detected.
timeout	Specifies that the operation measurement frequency should increase to the secondary frequency value if a one-way timeout is detected.
frequency	Secondary frequency to which an IP SLAs operation should change when a reaction condition occurs.

Command Default

The secondary frequency option is disabled.

Command Modes

MPLS parameters configuration (config-auto-ip-sla-mpls-params) VCCV configuration (config-ip-sla-vccv)

Command Modes

LSP ping configuration (config-sla-monitor-lspPing) LSP trace configuration (config-sla-monitor-lspTrace)

Note The configuration mode varies depending on the Cisco IOS release you are running and the operation type configured. See the “Usage Guidelines” section for more information.

Command History

Release	Modification
12.2(27)SBC	This command was introduced.

Release	Modification
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T. The **both** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	Support for MPLS Pseudo-Wire Emulation Edge-to-Edge (PWE3) services via Virtual Circuit Connectivity Verification (VCCV) was added.
12.2(33)SB	Support for MPLS Pseudo-Wire Emulation Edge-to-Edge (PWE3) services via Virtual Circuit Connectivity Verification (VCCV) was added.

Usage Guidelines

This command provides the capability to specify a secondary frequency for an IP SLAs operation. If the secondary frequency option is configured and a failure (such as a connection loss or timeout) is detected for a particular path, the frequency at which the path is remeasured will increase to the secondary frequency value (testing at a faster rate). When the configured reaction condition is met (such as N consecutive connection losses or N consecutive timeouts), an SNMP trap and syslog message can be sent and the measurement frequency will return to its original frequency value.

Note By default, if the secondary frequency option is not enabled, the frequency at which an operation remeasures a failed label switched path (LSP) is the same as the schedule period.

IP SLAs Operation Configuration Dependence on Cisco IOS Release

The Cisco IOS command used to begin configuration for an IP SLAs operation varies depending on the Cisco IOS release you are running (see the Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release table). Note that if you are configuring an IP SLAs LSP Health Monitor operation, see the Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release table for information on Cisco IOS release dependencies. You must configure the type of IP SLAs operation (such as LSP ping) before you can configure any of the other parameters of the operation.

The configuration mode for the **secondary-frequency** command varies depending on the Cisco IOS release you are running and the operation type configured. For example, if you are running Cisco IOS Release 12.4(6)T and the LSP ping operation type is configured (without using the LSP Health Monitor), you would enter the **secondary-frequency** command in LSP ping configuration mode (config-sla-monitor-lspPing) within IP SLA configuration mode.

Table 10: Command Used to Begin Configuration of an IP SLAs Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(4)T, 12.0(32)SY, 12.2(33)SRB, 12.2(33)SB, or later releases	**ip sla**	IP SLA configuration
12.3(14)T, 12.4, 12.4(2)T, 12.2(31)SB2, or 12.2(33)SXH	**ip sla monitor**	IP SLA monitor configuration

Table 11: Command Used to Begin Configuration of an IP SLAs LSP Health Monitor Operation Based on Cisco IOS Release

Cisco IOS Release	Global Configuration Command	Command Mode Entered
12.4(6)T, 12.0(32)SY, 12.2(31)SB2, 12.2(33)SRB, 12.2(33)SXH, or later releases	**auto ip sla mpls-lsp-monitor**	Auto IP SLA MPLS configuration

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, LSP Health Monitor operation 1 is configured to automatically create IP SLAs LSP ping operations for all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN routing and forwarding (VRF) instances associated with the source Provider Edge (PE) router. The secondary frequency option is enabled for both connection loss and timeout events, and the secondary frequency is set to 10 seconds.

```
mpls discovery vpn interval 60
mpls discovery vpn next-hop
!
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 timeout 1000
 scan-interval 1
 secondary-frequency both 10
 delete-scan-factor 2
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type
consecutive 3 action-type trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react timeout threshold-type consecutive
 3 action-type trapOnly
ip sla logging traps
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.

session-timeout (LSP discovery)

To set the amount of time the label switched path (LSP) discovery process for a Cisco IOS IP Service Level Agreements (SLAs) LSP Health Monitor operation waits for a response to its LSP discovery request for a particular Border Gateway Protocol (BGP) next hop neighbor, use the **session-timeout** command in auto IP SLA MPLS LSP discovery parameters configuration mode. To return to the default value, use the **no** form of this command.

session-timeout *seconds*

no session-timeout

Syntax Description

seconds	The amount of time (in seconds) an LSP Health Monitor operation waits for a response to its LSP discovery request. The default is 120.

Command Default

120 seconds

Command Modes

Auto IP SLA MPLS LSP discovery parameters configuration (config-auto-ip-sla-mpls-lpd-params)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Before an LSP discovery group is created for a particular BGP next hop neighbor, the LSP Health Monitor must receive a response to its LSP discovery request for that BGP next hop neighbor. If no response is received within the specified time limit, the LSP discovery process is not performed for that particular BGP next hop neighbor.

Use the **path-discover** command to enable the LSP discovery option for an IP SLAs LSP Health Monitor operation and enter auto IP SLA MPLS LSP discovery parameters configuration mode.

Examples

The following example shows how to configure operation parameters, proactive threshold monitoring, and scheduling options using the LSP Health Monitor. In this example, the LSP discovery option is enabled for LSP Health Monitor operation 1. Operation 1 is configured to automatically create IP SLAs LSP ping operations for the equal-cost multipaths to all Border Gateway Protocol (BGP) next hop neighbors in use by all VPN

routing and forwarding (VRF) instances associated with the source Provider Edge (PE) router. The timeout value for the LSP discovery requests is set to 60 seconds.

```
auto ip sla mpls-lsp-monitor 1
 type echo ipsla-vrf-all
 path-discover
!
 maximum-sessions 2
 session-timeout 60
 interval 2
 timeout 4
 force-explicit-null
 hours-of-statistics-kept 1
 scan-period 30
!
auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 frequency 100 start-time now
!
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd tree-trace action-type
trapOnly
auto ip sla mpls-lsp-monitor reaction-configuration 1 react lpd lpd-group retry 3 action-type
 trapOnly
```

Related Commands

Command	Description
auto ip sla mpls-lsp-monitor	Begins configuration for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS configuration mode.
path-discover	Enables the LSP discovery option for an IP SLAs LSP Health Monitor operation and enters auto IP SLA MPLS LSP discovery parameters configuration mode.

service performance

To begin configuring an IP Service Level Agreements (SLAs) service performance operation and enter IP SLA service performance configuration mode, use the **service-performance** command in IP SLA configuration mode.

service performance type *type* **dest-mac-addr** *mac-address* **interface** *interface* **service instance** *id*

Syntax Description

type *type*	Specifies a type for the service performance operation. The following keyword is valid for *type*: **ethernet**
dest-mac-addr *mac-address*	Identifies the destination device by it's MAC address. The format is H.H.H, where H is a hexadecimal value.
interface *interface*	Specifies the destination interface for the operation. The format for *interface* is *type number*.
service instance *id*	Specifies the Ethernet service instance for the operation.

Command Default

A service performance operation is not configured.

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
15.3(2)S	This command was introduced.

Usage Guidelines

Use this command to configure an IP SLAs service performance operation and enter service performance configuration mode for defining the parameters for a single service performance test stream.

You must first configure the service instance for this operation by using the **service instance** command.

To configure passive measurement mode, do not configure a traffic profile for this service performance operation. Passive measurement mode means that the operation does not generate live traffic and only collects statistics for the destination device configured for the operation.

To change the operation type of an existing IP SLAs operation, you must first delete the IP SLAs operation by using the **no ip sla** command and then reconfigure the operation with the new operation type.

Examples

The following sample output is the default configuration for a passive-measurement service performance operation:

```
sla-asr901-1# show ip sla configuration 10
IP SLAs Infrastructure Engine-III
Entry number: 10
Service Performance Operation
Type: ethernet
Destination
MAC Address: 4055.398d.8bd2
VLAN:
Interface: GigabitEthernet0/0
Service Instance: 10
EVC Name:
Duration Time: 30
Interval Buckets: 1

Signature:

Description:

Measurement Type:
 none
Direction: internal

Profile Traffic:
Direction: internal
CIR: 0
EIR: 0
CBS: 0
EBS: 0
Burst Size: 0
Burst Duration: 0
Inter Burst Interval: 0
Rate Step (kbps):

Profile Packet:
Inner COS: Not Set
Outer COS: Not Set
Inner VLAN: Not Set
Outer VLAN: Not Set
Source MAC Address: 0000.0000.0000
EtherType: default
Packet Size: 64
.
.
.
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
profile traffic	Configures a traffic profile for generating traffic.
service instance	Configures a service instance for an EFP.
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or a specified operation.