IP Service Level Agreements Commands

This module describes the Cisco IOS XR Software commands to implement IP service level agreements for system monitoring on the router.

For detailed information about IP service level agreements concepts, configuration tasks, and examples, see the *Implementing IP Service Level Agreements* chapter in the *System Monitoring Configuration Guide for Cisco 8000 Series Routers*.

access-list

To specify an access-list name to filter provider edge (PE) addresses to restrict operations that are automatically created by MPLS LSP monitor (MPLSLM) instance, use the **access-list** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

access-list *acl-name*
no access-list

Syntax Description

acl-name	Filters an access-list name.

Command Default

No access list is configured by default.

Command Modes

IP SLA MPLS LSP monitor ping configuration

IP SLA MPLS LSP monitor trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Access-list changes are processed before the scan interval expires to display a planned list of changes in the scan-queue.

Note There is no verification check between the access list and the IPSLA configuration.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **access-list** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# access-list ipsla
```

action (IP SLA)

To specify what action or combination of actions the operation performs when you configure the **react** command or when threshold events occur, use the **action** command in the appropriate configuration mode. To clear action or combination of actions (no action can happen), use the **no** form of this command.

action { **logging** | **trigger** }
no action { **logging** | **trigger** }

Syntax Description

logging	Sends a logging message when the specified violation type occurs for the monitored element. The IP SLA agent generates a syslog and informs SNMP. Then, it is up to the SNMP agent to generate a trap or not.
trigger	Determines that the operation state of one or more target operations makes the transition from pending to active when the violation conditions are met. The target operations to be triggered are specified using the **ipsla reaction trigger** command. A target operation continues until its life expires, as specified by the lifetime value of the target operation. A triggered target operation must finish its life before it can be triggered again.

Command Default

None

Command Modes

IP SLA reaction condition configuration

IP SLA MPLS LSP monitor reaction configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

For the **action** command to occur for threshold events, the threshold type must be defined. Absence of threshold type configuration is considered if the threshold check is not activated.

When the **action** command is used from IP SLA MPLS LSP monitor reaction configuration mode, only the **logging** keyword is available.

If the **action** command is used in IP SLA operation mode, the action defined applies to the specific operation being configured. If the **action** command is used in IP SLA MPLS LSP monitor mode, the action defined applies to all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **action** command with the **logging** keyword:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react connection-loss
Router(config-ipsla-react-cond)# action logging
```

The following example shows how to use the **action** command from the IP SLA MPLS LSP monitor reaction configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# reaction monitor 1
Router(config-ipsla-mplslm-react)# react connection-loss
Router(config-ipsla-mplslm-react-cond)# action logging
```

ageout

To specify the number of seconds to keep the operation in memory when it is not actively collecting information, use the **ageout** command in IP SLA schedule configuration mode. To use the default value so that the operation will never age out, use the **no** form of this command.

ageout *seconds*
no ageout

Syntax Description

seconds	Age-out interval in seconds. The value 0 seconds means that the collected data is not aged out. Range is 0 to 2073600.

Command Default

The default value is 0 seconds (never aged out).

Command Modes IP SLA schedule configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples The following example shows how to use the **ageout** command:

```
Rouuter# configure
Rouuter(config)# ipsla
Rouuter(config-ipsla)# schedule operation 1
Rouuter(config-ipsla-sched)# ageout 3600
```

buckets (history)

To set the number of history buckets that are kept during the lifetime of the IP SLA operation, use the **buckets** command in IP SLA operation history configuration mode. To use the default value, use the **no** form of this command.

buckets *buckets*
no buckets

Syntax Description

buckets	Number of history buckets that are kept during the lifetime of an IP SLA operation. Range is 1 to 60.

Command Default The default value is 15 buckets.

Command Modes IP SLA operation history configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines The **buckets** command is supported only to configure the following operations:

- IP SLA ICMP path-echo
- IP SLA ICMP echo

- IP SLA UDP echo

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **buckets** command in IP SLA UDP echo configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp echo
Router(config-ipsla-udp-echo)# history
Router(config-ipsla-op-hist)# buckets 30
```

buckets (statistics hourly)

To set the number of hours for which statistics are kept, use the **bucket** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

buckets *hours*
no buckets

Syntax Description

hours	Number of hours for which statistics are maintained for the IP SLA operations. Range is 0 to 25 in IP SLA operation statistics configuration mode, and 0 to 2 in IP SLA MPLS LSP monitor statistics configuration mode.

Command Default

The default value is 2.

Command Modes

IP SLA operation statistics configuration

IP SLA MPLS LSP monitor statistics configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **buckets** command with the *hours* argument is valid only for the **statistics** command with the **hourly** keyword.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to set the number of hours in which statistics are maintained for the IP SLA UDP jitter operation for the **buckets** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# statistics hourly
Router(config-ipsla-op-stats)# buckets 10
```

buckets (statistics interval)

To specify the maximum number of buckets in which the enhanced history statistics are kept, use the **buckets** command in IP SLA operation statistics configuration mode. To remove the statistics collection of the specified interval, use the **no** form of this command.

buckets *bucket-size*
no buckets

Syntax Description

bucket-size	The bucket size is when the configured bucket limit is reached. Therefore, statistics gathering for the operation ends. Range is 1 to 100. Default is 100.

Command Default

The default value is 100.

Command Modes

IP SLA operation statistics configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **buckets** command with the *bucket-size* argument is valid only for the **statistics** command with the **interval** keyword.

Examples

The following example shows how to collect statistics for a given time interval for the IP SLA UDP jitter operation for the **buckets** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# statistics interval 60
Router(config-ipsla-op-stats)# buckets 50
```

control disable

To disable the control packets, use the **control disable** command in the appropriate configuration mode. To use the control packets again, use the **no** form of this command.

control disable
no control disable

Syntax Description

This command has no keywords or arguments.

Command Default

Control packets are enabled by default.

Command Modes

IP SLA UDP echo configuration

IP SLA UDP jitter configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

When you configure the **control disable** command on the agent side, you need to configure a permanent port on the responder side or the operation returns a timeout error. If you configure the **control disable** command, a permanent port of the IP SLA Responder or some other functionality, such as the UDP echo server, is required on the remote device.

The **control disable** command is valid for operations that require a responder.

The IP SLA control protocol is disabled, which is used to send a control message to the IP SLA Responder prior to sending an operation packet. By default, IP SLA control messages are sent to the destination device to establish a connection with the IP SLA Responder.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **control disable** command in IP SLA UDP jitter configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# control disable
```

datasize request

To set the protocol data size in the request packet in the payload of an operation, use the **datasize request** command in the appropriate configuration mode. To reset the default data size, use the **no** form of this command.

datasize request *size*
no datasize request

Syntax Description

size Specifies the following ranges and default values that are protocol dependent:

- For a UDP jitter operation, range is 16 to 1500 B.
- For a UDP echo operation, range is 4 to 1500 B.
- For an ICMP echo operation, range is 0 to 16384 B.
- For an ICMP path-echo operation, range is 0 to 16384 B.
- For an ICMP path-jitter operation, range is 0 to 16384 B.
- For an MPLS LSP ping operation, range is 100 to 17986 B.

Command Default

For a UDP jitter operation, the default value is 32 B.

For a UDP echo operation, the default value is 16 B.

For an ICMP echo operation, the default value is 36 B.

For an ICMP path-echo operation, the default value is 36 B.

For an ICMP path-jitter operation, the default value is 36 B.

For an MPLS LSP ping operation, the default value is 100 B.

Command Modes

IP SLA UDP echo configuration

IP SLA UDP jitter configuration

IP SLA ICMP path-jitter configuration

IP SLA ICMP path-echo configuration

IP SLA ICMP echo configuration

IP SLA MPLS LSP ping configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **datasize request** command in IP SLA UDP jitter configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# datasize request 512
```

destination address (IP SLA)

To identify the address of the target device, use the **destination address** command in the appropriate configuration mode. To unset the destination address, use the **no** form of this command.

destination address *ipv4-address*
no destination address

Syntax Description

ipv4-address	IP address of the target device.

Command Default

None

Command Modes

IP SLA UDP echo configuration

IP SLA UDP jitter configuration

IP SLA ICMP path-jitter configuration

IP SLA ICMP path-echo configuration

IP SLA ICMP echo configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

You must specify the address of the target device. The configuration for the **destination address** command is mandatory for all operations.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to designate an IP address for the **destination address** command in IP SLA UDP jitter configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# destination address 192.0.2.12
```

destination port

To identify the port of the target device, use the **destination port** command in the appropriate configuration mode. To unset the destination port, use the **no** form of this command.

destination port *port*
no destination port

Syntax Description

port	Port number of the target device. Range is 1 to 65355.

Command Default

None

Command Modes

IP SLA UDP echo configuration

IP SLA UDP jitter configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **destination port** command is not supported when you configure an ICMP operation; it is supported only to configure UDP operations.

You must specify the port of the target device. The configuration for the **destination port** command is mandatory for both IP SLA UDP echo and IP SLA UDP jitter configurations.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to designate a port for the **destination port** command in IP SLA UDP jitter configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# destination port 11111
```

distribution count

To set the number of statistics distributions that are kept for each hop during the lifetime of the IP SLA operation, use the **distribution count** command in IP SLA operation statistics configuration mode. To use the default value, use the **no** form of this command.

distribution count *slot*
no distribution count

Syntax Description

slot	Number of statistics distributions that are kept. Range is 1 to 20. Default is 1.

Command Default

The default value is 1.

Command Modes

IP SLA operation statistics configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

In most situations, you do not need to change the number of statistics distributions kept or the time interval for each distribution. Only change these parameters when distributions are needed, for example, when performing statistical modeling of your network. To set the statistics distributions interval, use the **distribution interval** command in IP SLA operation statistics configuration mode. The total number of statistics distributions captured is the value set by the **distribution count** command times the value set by the **maximum hops** command times the value set by the **maximum path** command times the value set by the **buckets** command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to set the number of statistics distribution for the **distribution count** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
```

```
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# statistics hourly
Router(config-ipsla-op-stats)# distribution count 15
```

distribution interval

To set the time interval (in milliseconds) for each statistical distribution, use the **distribution interval** command in IP SLA operation statistics configuration mode. To use the default value, use the **no** form of this command.

distribution interval *interval*
no distribution interval

Syntax Description

interval	Number of milliseconds used for each statistics distribution that is kept. Range is 1 to 100. Default is 20.

Command Default

The default value is 20.

Command Modes

IP SLA operation statistics configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

In most situations, you do not need to change the number of statistics distributions kept or the time interval for each distribution. Only change these parameters when distributions are needed, for example, when performing statistical modeling of your network. To set the statistics distributions count, use the **distribution count** command in IP SLA operation statistics configuration mode. The total number of statistics distributions captured is the value set by the **distribution count** command times the value set by the **maximum hops** command times the value set by the **maximum path** command times the value set by the **buckets** command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to set the time interval for the **distribution interval** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# statistics hourly
Router(config-ipsla-op-stats)# distribution interval 50
```

exp

To specify the MPLS experimental field (EXP) value in the header of echo request packets, use the **exp** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

exp *exp-bits*
no exp

Syntax Description

exp-bits	Experimental field value in the header of an echo request packet. Valid values are from 0 to 7. Default is 0.

Command Default

The experimental field value is set to 0.

Command Modes

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

IP SLA MPLS LSP monitor ping configuration

IP SLA MPLS LSP monitor trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **exp** command to set the MPLS experimental field in the headers of echo request packets in an MPLS LSP ping or MPLS LSP trace operation. The experimental (EXP) field allows for eight different quality-of-service (QoS) markings that determine the treatment (per-hop behavior) that a transit LSR node gives to a request packet. You can configure different MPLS EXP levels for different operations to create differentiated levels of response.

If the **exp** command is used in IP SLA operation mode, it acts on the headers of echo request packets for the specific operation being configured. If the **exp** command is used in IP SLA MPLS LSP monitor mode, it acts on the headers of echo request packets for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **exp** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
```

```
Router(config-ipsla-op)# type mpls lsp trace
Router(config-ipsla-mpls-lsp-trace)# exp 5
```

The following example shows how to use the **exp** command in MPLS LSP monitor mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp trace
Router(config-ipsla-mplslm-lsp-trace)# exp 5
```

filter

To define the type of information that are kept in the history table for the IP SLA operation, use the **filter** command in IP SLA operation history configuration mode. To unset the history filter, use the **no** form of this command.

filter { **all** | **failures** }
no filter

Syntax Description

all	Stores history data for all operations, if set.
failures	Stores data for operations that failed, if set.

Command Default

The default is not to collect the history unless the **filter** command is enabled.

Command Modes

IP SLA operation history configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **filter** command is supported only to configure the following operations:

- IP SLA ICMP path-echo
- IP SLA ICMP echo
- IP SLA UDP echo

If you use the **no** form of the **filter** command, the history statistics are not collected.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **filter** command in IP SLA UDP echo configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp echo
Router(config-ipsla-udp-echo)# history
Router(config-ipsla-op-hist)# filter all
```

force explicit-null

To add an explicit null label to the label stack of an LSP when an echo request is sent, use the **force explicit-null** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

force explicit-null
no force explicit-null

Syntax Description

This command has no keywords or arguments.

Command Default

An explicit null label is not added.

Command Modes

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

IP SLA MPLS LSP monitor ping configuration

IP SLA MPLS LSP monitor trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **force explicit-null** command to force an unsolicited explicit null label to be added to the MPLS label stack of the LSP when an echo request packet is sent in an MPLS LSP ping or MPLS LSP trace operation.

If the **force explicit-null** command is used in IP SLA operation mode, it acts on the label stack of the LSP for the specific operation being configured. If the **force explicit-null** command is used in IP SLA MPLS LSP monitor mode, it acts on the label stack of all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

You cannot use the **force explicit-null** command if pseudowire is specified as the target to be used in an MPLS LSP ping operation.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **force explicit-null** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp trace
Router(config-ipsla-mpls-lsp-trace)# force explicit-null
```

frequency (IP SLA)

To set the frequency for probing, use the **frequency** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

frequency *seconds*
no frequency

Syntax Description

seconds	Rate at which the specific IP SLA operation is sent into the network. Range is 1 to 604800.

Command Default

If the **frequency** command is not used, the default value is 60 seconds.

In IP SLA MPLS LSP monitor schedule configuration mode, the default value is equal to the schedule period that is set using the **schedule period** command.

Command Modes

IP SLA UDP echo configuration

IP SLA UDP jitter configuration

IP SLA ICMP path-jitter configuration

IP SLA ICMP path-echo configuration

IP SLA ICMP echo configuration

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

IP SLA MPLS LSP monitor schedule configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

If this command is used in IP SLA MPLS LSP monitor schedule configuration mode, it represents the frequency for the schedule period. In other words, if the frequency is set to 1000 seconds and the schedule period is set to 600 seconds, every 1000 seconds the LSP operations are run. Each run takes 600 seconds. Use the **schedule period** command to specify the schedule period.

The frequency value must be greater than or equal to the schedule period.

This configuration is inherited automatically by all LSP operations that are created.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **frequency** command in IP SLA UDP jitter configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# frequency 300
```

The following example shows how to use the **frequency** command in IP SLA MPLS LSP monitor schedule configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# schedule monitor 1
Router(config-ipsla-mplslm-sched)# frequency 1200
Router(config-ipsla-mplslm-sched)# schedule period 600
```

history

To configure the history parameters for the IP SLA operation, use the **history** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

history [**buckets** *buckets* | **filter** { **all** | **failures** } | **lives** *lives*]
no history

Syntax Description

buckets	Sets the number of history buckets that are kept during the lifetime of the IP SLA operation.
buckets	Number of history buckets that are kept during the lifetime of an IP SLA operation. Range is 1 to 60.
filter	Defines the type of information that is kept in the history table for the IP SLA operation.
all	Stores history data for all operations, if set.
failures	Stores data for operations that failed, if set.
lives	Sets the number of lives that are maintained in the history table for an IP SLA operation.
lives	Number of lives that are maintained in the history table for an IP SLA operation. Range is 0 to 2.

Command Default

None

Command Modes

IP SLA UDP echo configuration

IP SLA UDP jitter configuration

IP SLA ICMP path-jitter configuration

IP SLA ICMP path-echo configuration

IP SLA ICMP echo configuration

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **history** command enters IP SLA operation history configuration mode in which you can configure more history configuration parameters.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **history** command in IP SLA UDP echo configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp echo
Router(config-ipsla-udp-echo)# history
Router(config-ipsla-op-hist)#
```

hw-timestamp disable

To disable hardware time stamp configuration, use the **hw-timestamp disable** command in the IP SLA configuration mode.

hw-timestamp disable

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

IP SLA configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
monitor	read, write

Example

The following example shows how to disable hardware time stamping:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# hw-timestamp disable
```

interval

To configure the refresh interval for MPLS label switched path (LSP) monitoring, use the **interval** command in IP SLA MPLS discovery VPN configuration mode. To use the default value, use the **no** form of this command.

interval *refresh-interval*
no interval

Syntax Description

refresh-interval	Specifies the time interval, in minutes, after which routing entries that are no longer valid are removed from the Layer 3 VPN discovery database. Range is 30 to 70560.

Command Default

The default refresh interval is 60 minutes.

Command Modes

IP SLA MPLS discovery VPN configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Note If the total number of routes is large, there is a negative impact on the performance during the refresh of the discovery database. Therefore, the value of the *refresh-interval* argument should be large enough that router performance is not affected. If there are a very large number of routes, we recommend that you set the value of the *refresh-interval* argument to be several hours.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **interval** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls discovery vpn
Router(config-ipsla-mpls-discovery-vpn)# interval 120
```

ipsla

To enter IP SLA configuration mode and configure IP Service Level Agreements, use the **ipsla** command in XR Config mode. To return to the default setting, use the **no** form of this command.

ipsla
no ipsla

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR Config mode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **ipsla** command enters IP SLA configuration mode where you can configure the various IP service level agreement options.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to enter IP SLA configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)#
```

key-chain

To configure the MD5 authentication for the IP SLA control message, use the **key-chain** command in IP SLA configuration mode. To unset the keychain name and not use MD5 authentication, use the **no** form of this command.

key-chain *key-chain-name*
no key-chain

Syntax Description

key-chain-name	Name of the keychain.

Command Default

No default values are defined. No authentication is used.

Command Modes

IP SLA configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

When you configure the **key-chain** command, you must also configure the **key chain** command in global configuration mode to provide MD5 authentication.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **ipsla key-chain** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# key-chain ipsla-keys
```

life

To specify the length of time to execute, use the **life** command in IP SLA schedule configuration mode. To use the default value, use the **no** form of this command.

life { **forever** *seconds* }
no life

Syntax Description

forever	Schedules the operation to run indefinitely.
seconds	Determines the number of seconds the operation actively collects information. Range is 1 to 2147483647. Default value is 3600 seconds (one hour).

Command Default

The default value is 3600 seconds.

Command Modes

IP SLA schedule configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **life** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# schedule operation 1
Router(config-ipsla-sched)# life forever
```

lives

To set the number of lives that are maintained in the history table for an IP SLA operation, use the **lives** command in IP SLA operation history configuration mode. To use the default value, use the **no** form of this command.

lives *lives*
no lives

Syntax Description

lives	Number of lives that are maintained in the history table for an IP SLA operation. Range is 0 to 2.

Command Default

The default value is 0 lives.

Command Modes

IP SLA operation history configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **lives** command is supported only to configure the following operations:

- IP SLA ICMP path-echo
- IP SLA ICMP echo
- IP SLA UDP echo

If you use the **no** form of the **lives** command, the history statistics are not collected.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **lives** command in IP SLA UDP echo configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp echo
Router(config-ipsla-udp-echo)# history
Router(config-ipsla-op-hist)# lives 2
```

local-ip

To configure the test-session parameters for TWAMP-light responder, use the **local-ip** command in the **ipsla responder twamp-light** mode. To remove the set configuration, use the **no** form of the command.

local-ip *local-ip-address* **local-port** *local-port* **remote-ip** *remote-ip-address* **remote-port** *remote-port* **vrf** [**default** | *vrf-name*]

Syntax Description

local-ip *local-ip-address*	Configure IPv4/IPv6 address of the interface on the local router
local-port *local-port*	Configure the UDP port number of the local router. Range is 1 - 65535
remote-ip *remote-ip-address*	Configure IPv4/IPv6 address of the interface on the remote router
remote-port *remote-port*	Configure the UDP port number of the remote router. Range is 1 - 65535
vrf [**default**	*vrf-name*]	Configure the VRF that the interface on the local router is part of

Command Default

None

Command Modes

IPSLA responder TWAMP-light configuration mode

Command History

Release	Modification
Release 7.3.2	This command is introduced.

Usage Guidelines No specific guidelines impact the use of this command.

Example

This example shows how to run the **responder** command in order to configure TWAMP responder:

```
Router(config)# ipsla
Router(config-ipsla)# responder twamp-light test-session 1
Router(config-twamp-light-def)# local-ip 192.0.2.10 local-port 13001 remote-ip 192.0.2.186
 remote-port 13002 vrf default
```

low-memory

low-memory *value*
no low-memory

Syntax Description

value	Low-water memory mark value. Range is 0 to 4294967295.

Command Default The default value is 20 MB (free memory).

Command Modes IP SLA configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines IP SLA ensures that the system provides the specified memory before adding new operations or scheduling the pending operation.

When the 0 value is used, no memory limitation is enforced.

Task ID

Task ID	Operations
monitor	read, write

Examples The following example shows how to use the **low-memory** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# low-memory 102400
```

lsp selector ipv4

To specify the local host IPv4 address used to select an LSP, use the **lsp selector ipv4** command in the appropriate configuration mode. To clear the host address, use the **no** form of this command.

lsp selector ipv4 *ip-address*
no lsp selector ipv4

Syntax Description

ip-address	A local host IPv4 address used to select the LSP.

Command Default

The local host IP address used to select the LSP is 127.0.0.1.

Command Modes

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

IP SLA MPLS LSP monitor ping configuration

IP SLA MPLS LSP monitor trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **lsp selector ipv4** command to force an MPLS LSP ping or MPLS LSP trace operation to use a specific LSP when there are multiple equal cost paths between provider edge (PE) routers. This situation occurs when transit label switching routers (LSRs) use the destination address in IP packet headers for load balancing.

The IPv4 address configured with the **lsp selector ipv4** command is the destination address in the User Datagram Protocol (UDP) packet sent as the MPLS echo request. Valid IPv4 addresses are defined in the subnet 127.0.0.0/8 and used to:

- Force the packet to be consumed by the router where an LSP breakage occurs.
- Force processing of the packet at the terminal point of the LSP if the LSP is intact.
- Influence load balancing during forwarding when the transit routers use the destination address in the IP header for load balancing.

If the **lsp selector ipv4** command is used in IP SLA operation mode, it acts on the MPLS echo requests for the specific operation being configured. If the **lsp selector ipv4** command is used in IP SLA MPLS LSP monitor mode, it acts on the MPLS echo requests for all operations associated with the monitored provider edge (PE) routers.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **lsp selector ipv4** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp trace
Router(config-ipsla-mpls-lsp-trace)# lsp selector ipv4 127.10.10.1
```

lsr-path

To specify a loose source routing path in which to measure the ICMP, use the **lsr-path** command in the appropriate configuration mode. To use a path other than the specified one, use the **no** form of this command.

lsr-path ipaddress1 [**ipaddress2** [**. . .** [**ipaddress8**]]]
no lsr-path

Syntax Description

ip address	IPv4 address of the intermediate node. Up to eight addresses can be entered.

Command Default

No path is configured.

Command Modes

IP SLA ICMP path-jitter configuration

IP SLA ICMP path-echo configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **lsr-path** command applies only to ICMP path-echo and ICMP path-jitter operation types.

You can configure up to a maximum of eight hop addresses by using the **lsr-path** command, as shown in the following example:

```
lsr-path ipaddress1 [ipaddress2 [... [ipaddress8]]]
```

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **lsr-path** command in IP SLA ICMP Path-echo configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type icmp path-echo
Router(config-ipsla-icmp-path-echo)# lsr-path 192.0.2.40
```

maximum hops

To set the number of hops in which statistics are maintained for each path for the IP SLA operation, use the **maximum hops** command in IP SLA operation statistics configuration mode. To use the default value, use the **no** form of this command.

maximum hops *hops*
no maximum hops

Syntax Description

hops	Number of hops for which statistics are maintained for each path. Range is 1 to 30. Default value is 16 for path operations; for example, *pathecho*.

Command Default

The default value is 16 hops.

Command Modes

IP SLA operation statistics configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **maximum hops** command is supported only when you configure path operations and the IP SLA ICMP path-echo operation.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to set the number of hops for the statistics for the **maximum** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type icmp path-echo
Router(config-ipsla-icmp-path-echo)# statistics hourly
Router(config-ipsla-op-stats)# maximum hops 20
```

maximum paths (IP SLA)

To set the number of paths in which statistics are maintained for each hour for an IP SLA operation, use the **maximum paths** command in IP SLA operation statistics configuration mode. To use the default value, use the **no** form of this command.

maximum paths *paths*

no maximum paths

Syntax Description

paths	Number of paths for which statistics are maintained for each hour. Range is 1 to 128. Default value is 5 for path operations; for example, *pathecho*.

Command Default

The default value is 5 paths.

Command Modes

IP SLA operation statistics configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **maximum paths** command is supported only when you configure path operations and the IP SLA ICMP path-echo operation.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to set the number of paths for the statistics for the **maximum paths** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type icmp path-echo
Router(config-ipsla-icmp-path-echo)# statistics hourly
Router(config-ipsla-op-stats)# maximum paths 20
```

monitor (IP SLA)

To configure an MPLS LSP monitor instance, use the **monitor** command in IP SLA LSP monitor configuration mode. To remove the monitor instance, use the **no** form of this command.

monitor *monitor-id*
no monitor [*monitor-id*]

Syntax Description

monitor-id	Number of the IP SLA LSP monitor instance to be configured. Range is 1 to 2048.

Command Default

No monitor instance is configured.

Command Modes

IP SLA LSP monitor configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **monitor** command enters IP SLA MPLS LSP monitor configuration mode so that you can set the desired monitor type for all operations associated with the monitored provider edge (PE) routers.

To remove all monitor instances, use the **no monitor** command with no argument.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **monitor** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)#
```

mpls discovery vpn

To configure MPLS label switched path (LSP) provider edge (PE) router discovery, use the **mpls discovery vpn** command in IP SLA configuration mode. To use the default value, use the **no** form of this command.

mpls discovery vpn [**interval** *interval*]
no mpls discovery vpn

Syntax Description

interval	Configures the refresh interval for MPLS label switched path (LSP) monitoring.

Command Default

None

Command Modes

IP SLA configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **mpls discovery vpn** command to configure provider edge (PE) router discovery. PE Discovery discovers the LSPs used to reach every routing next hop. Routing entities are stored in a Layer 3 VPN discover database.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to enter IP SLA MPLS discovery VPN mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls discovery vpn
Router(config-ipsla-mpls-discovery-vpn)#
```

mpls lsp-monitor

To configure MPLS label switched path (LSP) monitoring, use the **mpls lsp-monitor** command in IP SLA configuration mode. To use the default value, use the **no** form of this command.

mpls lsp-monitor
no mpls lsp-monitor

Syntax Description

None

Command Default

None

Command Modes

IP SLA configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **mpls lsp-monitor** command to configure MPLS LSP PE monitoring on the router. This provides a means to configure all operations associated with the monitored provider edge (PE) routers. The configuration is inherited by all LSP operations that are created automatically by the PE discovery.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to enter IP SLA MPLS LSP monitor mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)#
```

operation

To configure an IP SLA operation, use the **operation** command in IP SLA configuration mode. To remove the operation, use the **no** form of this command.

operation *operation-number*
no operation *operation-number*

Syntax Description

operation-number	Operation number. Range is 1 to 2048.

Command Default

None

Command Modes

IP SLA configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the IP SLA **operation** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)#
```

output interface

To specify the echo request output interface to be used for LSP ping or LSP trace operations, use the **output interface** command in IP SLA MPLS LSP ping or IP SLA MPLS LSP trace configuration mode. To return the output interface to the default, use the **no** form of this command.

output interface *type interface-path-id*
no output interface

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.

interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values.

Command Modes

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

IP SLA MPLS LSP monitor ping configuration

IP SLA MPLS LSP monitor trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **output interface** command to help monitor path-to-target over the path if there are some ECMP routes in a topology.

You cannot use the **output interface** command if pseudowire is specified as the target to be used in an MPLS LSP ping operation.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **output interface** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls ls output interface pos 0/1/0/0
```

output nexthop

To specify the next-hop address to be used for a Label Switched Path (LSP) ping or LSP trace operations, use the **output nexthop** command in the appropriate configuration mode. To return the output next hop to the default, use the **no** form of this command.

output nexthop *ip-address*
no output nexthop

Syntax Description

ip-address	IP address of the next hop.

Command Default

No default behavior or values

Command Modes

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

IP SLA MPLS LSP monitor ping configuration

IP SLA MPLS LSP monitor trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

When LSP Path Discovery (LPD) is enabled, the next-hop IP address is also used to filter out the paths that are not associated with the specified next-hop address.

Note After you configure the output next hop, you must also configure the output interface.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **output nexthop** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp trace
Router(config-ipsla-mpls-lsp-trace)# output nexthop 10.1.1.1
```

packet count

To specify the number of packets that are to be transmitted during a probe, such as a sequence of packets being transmitted for a jitter probe, use the **packet count** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

packet count *count*
no packet count

Syntax Description

count	Number of packets to be transmitted in each operation. Range for a UDP jitter operation is 1 to 60000. Range for an ICMP path-jitter operation is 1 to 100.

Command Default The default packet count is 10.

Command Modes IP SLA UDP jitter configuration

IP SLA ICMP path-jitter configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples The following example shows how to use the **packet count** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# packet count 30
```

packet interval

To specify the interval between packets, use the **packet interval** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

packet interval *interval*
no packet interval

Syntax Description

interval	Interpacket interval in milliseconds. Range is 1 to 60000 (in milliseconds).

Command Default The default packet interval is 20 ms.

Command Modes IP SLA UDP jitter configuration

IP SLA ICMP path-jitter configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **packet interval** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# packet interval 30
```

path discover

To enable path discovery and enter MPLS LSP monitor (MPLSLM) LPD submode, use the **path discover** command in IP SLA MPLS LSP monitor ping configuration mode. To use the default value, use the **no** form of this command.

path discover
no path discover

Syntax Description

None

Command Default

No default behavior or values

Command Modes

IP SLA MPLS LSP monitor ping configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to enter path discover submode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
```

```
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# path discover
Router(config-ipsla-mplslm-lpd)#
```

path discover echo

To configure MPLS LSP echo parameters, use the **path discover** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

path discover echo { **interval** *time* | **maximum lsp selector ipv4** *host address* | **multipath bitmap size** *size* | **retry** *count* | **timeout** *value* }
no path discover echo { **interval** *time* | **maximum lsp selector ipv4** *host address* | **multipath bitmap size** *size* | **retry** *count* | **timeout** *value* }

Syntax Description

interval *time*	Configures the interval (in milliseconds) between MPLS LSP echo requests sent during path discovery. Range is 0 to 3600000. Default is 0.
maximum lsp selector ipv4 *host-address*	Configures a local host IP address (127.*x*.*x*.*x*) that is the maximum selector value to be used during path discovery. Default is 127.255.255.255.
multipath bitmap size *size*	Configures the maximum number of selectors sent in the downstream mapping of an MPLS LSP echo request during path discovery. Range is 1 to 256. Default is 32.
retry *count*	Configures the number of timeout retry attempts for MPLS LSP echo requests sent during path discovery. Range is 0 to 10. Default is 3.
timeout *value*	Configures the timeout value (in seconds) for MPLS LSP echo requests sent during path discovery. Range is 1 to 3600. Default is 5.

Command Default

interval *time*: 0

maximum lsp selector ipv4 *host address*: 127.255.255.255

multipath bitmap size *size : 32*

retry *count*: 3

timeout *value*: 5

Command Modes

Path discover configuration

MPLS LSP ping configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

A retry occurs when either an echo reply was not received on time for an outstanding echo request, or when no selectors are found for a given path by a transit router.

When a selector value is configured in MPLSLM configuration mode, the maximum selector specified must be larger than that value. In such a scenario, the range of selectors used for path discovery is set by the two values.

When the **interval** *time* is zero, a new echo request is sent after the previous echo retry was received.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to configure the path discover echo interval:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# path discover
Router(config-ipsla-mplslm-lsp-lpd)# echo interval 777
```

path discover path

To configure MPLS LSP path parameters, use the **path discover path** command in MPLS LSP monitor (MPLSLM) LPD configuration submode. To use the default value, use the **no** form of this command.

path discover path { **retry** *range* | **secondary frequency** { **both** | **connection-loss** | **timeout** } *value* }
no path-discover path

Syntax Description

retry *range*	Configures the number of attempts to be performed before declaring a path as down. Default is 1 (LSP group will not retry to perform the echo request if the previous attempt fails). Range is 1 to 16.
secondary frequency	Configures a secondary frequency to use after a failure condition (that is, a connection-loss or timeout) occurs.
both	Enable secondary frequency for a timeout and connection loss.
connection-loss	Enable secondary frequency for only a connection loss.
timeout	Enable secondary frequency for only a timeout.
value	Frequency value range is 1 to 604800.

Command Default

None

Command Modes

MPLSLM LPD configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

In the event of a path failure, the secondary frequency value is used instead of the normal frequency value. The normal frequency value is determined by a frequency value or schedule period value, and the LSP operations are scheduled to start periodically at this interval. By default, the secondary frequency value is disabled. When failure condition disappears, probing resumes at the regular frequency.

Note *The* **secondary** *command works in tandem with the* **retry** *keyword. Both must be configured.*

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to configure MPLS LSP path parameters:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# path discover
Router(config-ipsla-mplslm-lsp-lpd)# path retry 12
Router(config-ipsla-mplslm-lsp-lpd)# path secondary frequency both 10
```

path discover scan

To configure MPLS LSP scan parameters, use the **path discover scan** command in MPLS LSP monitor (MPLSLM) LPD configuration submode. To use the default value, use the **no** form of this command.

path discover scan period *value*
no path discover scan period *value*

Syntax Description

period *value*	Configures the time (in minutes) between consecutive cycles of path discovery requests per MPLSLM instance. Range is 0 to 7200. Default is 5.

Command Default

period *value : 5*

Command Modes

MPLSLM LPD configuration submode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

MPLSLM instances periodically trigger path discovery requests for LSP groups. At certain intervals, an MPLSLM instance begins triggering path discovery requests for each group in ascending order (determined by group ID). By default, the path discovery requests are triggered sequentially, although some concurrency may occur if the session limit value is greater than 1. The cycle concludes when the last LSP group finishes path discovery.

If the duration of the discovery cycle is larger than the scan period, a new cycle starts as soon as the previous one completes.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to configure the path discovery scan period value:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# path discover
Router(config-ipsla-mplslm-lsp-lpd)# scan period 2
```

path discover session

To configure MPLS LSP session parameters, use the **path discover session** command in MPLS LSP monitor (MPLSLM) LPD configuration submode. To use the default value, use the **no** form of this command.

path discover session { **limit** *value* | **timeout** *value* }
no path discover session { **limit** *value* | **timeout** *value* }

Syntax Description

limit *value*	Configures the number of concurrent active path discovery requests the MPLSLM instance submits to the LSPV server. Range is 1 to 15. Default is 1.
timeout *value*	Configures the time (in seconds) the MPLSLM instance will wait for the result of a path discovery request submitted to the LSPV server. Range is 1 to 900. Default is 120.

Command Default

limit *value : 1*

timeout *value : 120*

Command Modes

MPLSLM LPD configuration submode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

An MPLSLM instance considers the path discovery as a failure when it receives no response within the configured timeout configuration value.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to configure the path discovery session timeout value:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# path discover
Router(config-ipsla-mplslm-lsp-lpd)# session timeout 22
```

react

To specify an element to be monitored for a reaction, use the **react** command in the appropriate configuration mode. To remove the specified reaction type, use the **no** form of this command.

react { **connection-loss** | **jitter-average** [**dest-to-source** | **source-to-dest**] | **packet-loss** { **dest-to-source** | **source-to-dest** } | **rtt** | **timeout** | **verify-error** }
no react { **connection-loss** | **jitter-average** [**dest-to-source** | **source-to-dest**] | **packet-loss** { **dest-to-source** | **source-to-dest** } | **rtt** | **timeout** | **verify-error** }

Syntax Description

connection-loss	Specifies that a reaction occurs if there is a connection-loss for the monitored operation.
jitter-average [**dest-to-source** | **source-to-dest**]	Specifies that a reaction occurs if the average round-trip jitter value violates the upper threshold or lower threshold. The following options are listed for the **jitter-average** keyword: • **dest-to-source**—(Optional) Specifies the jitter average destination to source (DS). • **source-to-dest**—(Optional) Specifies the jitter average source to destination (SD).

packet-loss {**dest-to-source** | **source-to-dest**}	Specifies the reaction on packet loss value violation. The following options are listed for the **packet-loss** keyword: • **dest-to-source**—(Optional) Specifies the packet loss destination to source (DS) violation. • **source-to-dest**—(Optional) Specifies the packet loss source to destination (SD) violation.
rtt	Specifies that a reaction occurs if the round-trip value violates the upper threshold or lower threshold.
timeout	Specifies that a reaction occurs if there is a timeout for the monitored operation.
verify-error	Specifies that a reaction occurs if there is an error verification violation.

Command Default

If there is no default value, no reaction is configured.

Command Modes

IP SLA reaction configuration

IP SLA MPLS LSP monitor reaction configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

For the **connection-loss** keyword, **jitter-average** keyword, and **rtt** keyword, the reaction does not occur when the value violates the upper or the lower threshold. The reaction condition is set when the upper threshold is passed, and it is cleared when values go below the lower threshold.

For the **connection-loss** keyword and **verify-error** keyword, thresholds do not apply to the monitored element.

For the **jitter-average** keyword, **packet-loss** keyword, and **rtt** keyword, if the upper threshold for react 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 is 6000 + 6000 + 5000=17000/3 = 5667—therefore violating the 5000-ms upper threshold. The threshold type average must be configured when setting the type. These keywords are not available if connection-loss, timeout, or verify-error is specified as the monitored element, because upper and lower thresholds do not apply to these options.

In IP SLA MPLS LSP monitor reaction configuration mode, only the **connection-loss** and **timeout** keywords are available. If the **react** command is used in IP SLA MPLS LSP monitor reaction configuration mode, it configures all operations associated with the monitored provider edge (PE) routers. The configuration is inherited by all LSP operations that are created automatically by the PE discovery.

This table lists the Supported Reaction Configuration, by IP SLA Operation.

Table 1: Supported Reaction Configuration, by IP SLA Operation

Operation	ICMP Echo	Path Echo	UDP Jitter	UDP Echo	ICMP Path Jitter	MPLS LSP Ping	MPLS LSP Trace
Failure	--	--	--	--	--	--	--
RTT	Y	Y	Y	Y	Y	Y	Y

Operation	ICMP Echo	Path Echo	UDP Jitter	UDP Echo	ICMP Path Jitter	MPLS LSP Ping	MPLS LSP Trace
RTTAvg	--	--	--	--	--	--	--
Timeout	Y	Y	Y	Y	Y	Y	Y
connectionLoss	--	--	Y	Y	--	Y	Y
verifyError	--	--	Y	Y	--	--	--
jitterSDAvg	--	--	Y	--	--	--	--
jitterDSAvg	--	--	Y	--	--	--	--
jitterAvg	--	--	Y	--	--	--	--
PacketLossDS	--	--	Y	--	--	--	--
PacketLossSD	--	--	Y	--	--	--	--
PacketLoss	--	--	Y	--	--	--	--

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **react** command with the **connection-loss** keyword:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react connection-loss
Router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **jitter-average** keyword:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react jitter-average
Router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **packet-loss** keyword:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react packet-loss dest-to-source
Router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **rtt** keyword:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react rtt
Router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **timeout** keyword:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react timeout
Router(config-ipsla-react-cond)#
```

The following example shows how to use the **react** command with the **verify-error** keyword:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react verify-error
Router(config-ipsla-react-cond)#
```

react lpd

To specify that a reaction should occur if there is an LSP Path Discovery (LPD) violation, use the **react lpd** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

react lpd { **lpd-group** | **tree-trace** } **action logging**
no react lpd { **lpd-group** | **tree-trace** }

Syntax Description

lpd-group	Specifies that a reaction should occur if there is a status violation for the monitored LPD group.
tree-trace	Specifies that a reaction should occur if there is a path discovery violation for the monitored LPD group.
action	Configures the action to be taken on threshold violation.
logging	Specifies the generation of a syslog alarm on threshold violation.

Command Default

None

Command Modes

IP SLA MPLS LSP monitor configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

A status violation for a monitored LPD group happens when the Label Switched Path (LSP) group status changes (with the exception of the status change from the initial state).

A path discovery violation for the monitored LPD group happens when path discovery to the target PE fails, or successful path discovery clears such a failure condition.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to specify that a reaction should occur if there is a status violation for the monitored LPD group:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# reaction monitor 1
Router(config-ipsla-mplslm-react)# react lpd lpd-group action logging
```

reaction monitor

To configure MPLS label switched path (LSP) monitoring reactions, use the **reaction monitor** command in IP SLA MPLS LSP monitor configuration mode. To remove the reaction so that no reaction occurs, use the **no** form of this command.

reaction monitor *monitor-id*
no reaction monitor [*monitor-id*]

Syntax Description

monitor-id	Number of the IP SLA MPLS LSP monitor instance for the reactions to be configured. Range is 1 to 2048.

Command Default

No reaction is configured.

Command Modes

IP SLA MPLS LSP monitor configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **reaction monitor** command enters IP SLA LSP monitor reaction configuration mode so that you can set the desired threshold and action in the event of a connection loss or timeout.

To remove all reactions, use the **no reaction monitor** command with no *monitor-id* argument.

The **reaction monitor** command configures reactions for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **reaction operation** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# reaction monitor 1
Router(config-ipsla-mplslm-react)#
```

reaction operation

To configure certain actions that are based on events under the control of the IP SLA agent, use the **reaction operation** command in IP SLA configuration mode.To remove the reaction so that no reaction occurs, use the **no** form of this command.

reaction operation *operation-id*
no reaction operation *operation-id*

Syntax Description

operation-id	Number of the IP SLA operation for the reactions to be configured. Range is 1 to 2048.

Command Default

No reaction is configured.

Command Modes

IP SLA configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **reaction operation** command:

```
Router# configure
Router(config)# ipsla
```

```
Router(config-ipsla)# reaction operation 1
Router(config-ipsla-react)#
```

reaction trigger

To define a second IP SLA operation to make the transition from a pending state to an active state when one of the trigger-type options is defined with the **reaction operation** command, use the **reaction trigger** command in IP SLA configuration mode. To remove the reaction trigger when the *triggering-operation* argument does not trigger any other operation, use the **no** form of this command.

reaction trigger *triggering-operation triggered-operation*
no reaction trigger *triggering-operation triggered-operation*

Syntax Description

triggering-operation	Operation that contains a configured action-type trigger and can generate reaction events. Range is 1 to 2048.
triggered-operation	Operation that is started when the *triggering-operation* argument generates a trigger reaction event. Range is 1 to 2048.

Command Default

No triggered operation is configured.

Command Modes

IP SLA configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Both the *triggering-operation* and *triggered-operation* arguments must be configured. The triggered operation must be in the pending state.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **ipsla reaction trigger** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction trigger 1 2
```

reply dscp

To specify the differentiated services codepoint (DSCP) value used in echo reply packets, use the **reply dscp** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

reply dscp *dscp-bits*
no reply dscp

Syntax Description

dscp-bits	Differentiated services codepoint (DSCP) value for an echo reply packet. Valid values are from 0 to 63. Reserved keywords such as EF (expedited forwarding) and AF11 (assured forwarding class AF11) can be specified instead of numeric values.

Command Default

No default behavior or values

Command Modes

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

IP SLA MPLS LSP monitor ping configuration

IP SLA MPLS LSP monitor trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **reply dscp** command to set the DCSP value used in the headers of IPv4 UDP packets sent as echo replies in an MPLS LSP ping or MPLS LSP trace operation.

The DSCP value consists of the six most significant bits of the 1-byte IP type of service (ToS) field. These bits determine the quality-of-service (QoS) treatment (per-hop behavior) that an transit LSR node gives to an echo reply packet. For information about how packets are classified and processed depending on the value you assign to the 6-bit DSCP field, refer to “The Differentiated Services Model (DiffServ)” at the following URL:

http://www.cisco.com/en/US/products/ps6610/products_data_sheet09186a00800a3e30.html

If the **reply dscp** command is used in IP SLA operation mode, it acts on the headers of echo replies for the specific operation being configured. If the **reply dscp** command is used in IP SLA MPLS LSP monitor mode, it acts on the headers of echo replies for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **reply dscp** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp ping
Router(config-ipsla-mpls-lsp-ping)# reply dscp 5
```

reply mode

To specify how to reply to echo requests, use the **reply mode** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

reply mode { **control-channel** | **router-alert** }
no reply mode

Syntax Description

control-channel	Sets echo requests to reply by way of a control channel. **Note** This option is available only in IP SLA MPLS LSP ping configuration mode.
router-alert	Sets echo requests to reply as an IPv4 UDP packet with IP router alert.

Command Default

The default reply mode for an echo request packet is an IPv4 UDP packet without IP router alert set.

Command Modes

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

IP SLA MPLS LSP monitor ping configuration

IP SLA MPLS LSP monitor trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **reply mode** command with the **control-channel** keyword to send echo reply packets by way of a control channel in an MPLS LSP ping operation. If the target is not set to pseudowire, the configuration of the **control-channel** keyword is rejected. Refer to the **target pseudowire** command for information about setting the target.

Use the **reply mode** command with the **router-alert** keyword to set the reply mode of echo reply packets in an MPLS LSP ping or MPLS LSP trace operation. After you enter this command, echo reply packets are set to reply as an IPv4 UDP packet with the IP router alert option in the UDP packet header.

If the **reply mode** command is used in IP SLA operation mode, it sets the reply mode of echo reply packets for the specific operation being configured. If the **reply mode** command is used in IP SLA MPLS LSP monitor mode, it sets the reply mode of echo reply packets for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

The router-alert reply mode forces an echo reply packet to be specially handled by the transit LSR router at each intermediate hop as it moves back to the destination. Because this reply mode is more expensive, it is recommended only if the headend router does not receive echo replies using the default reply mode.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **reply mode** command with the **router-alert** keyword:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp trace
Router(config-ipsla-mpls-lsp-trace)# reply mode router-alert
```

The following example shows how to use the **reply mode** command with the **control-channel** keyword:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp ping
Router(config-ipsla-mpls-lsp-ping)# target pseudowire 192.168.1.4 4211
Router(config-ipsla-mpls-lsp-ping)# reply mode control-channel
```

responder

To configure the responder for IP SLA, use the **responder** command in the **ipsla** mode. To remove the set configuration, use the **no** form of the command.

responder [**twamp** | [**twamp-light** **test-session** *test-session-id*]] [**timeout** *timeout-value*]

responder twamp [**timeout** *timeout-value*]

Syntax Description

twamp	Configure TWAMP responder
twamp-light	Configure TWAMP-light responder
test-session *test-session-id*	Configure TWAMP-light test-session id. Range is 1 - 65535
timeout *timeout-value*	Configure the inactivity timeout period (in seconds) Range is 1 - 604800 For TWAMP, the range is 1 - 604800. For TWAMP-light, the range is 60 - 86400

Command Default

Default timeout for TWAMP responder is 900 seconds.

By default, there is no timeout for TWAMP-light responder.

Command Modes

IPSLA configuration mode

Command History

Release	Modification
Release 7.3.2	This command is introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Example

This example shows how to configure the TWAMP responder:

```
Router(config)# ipsla
Router(config-ipsla)# responder twamp timeout 100
```

This example shows how to configure the TWAMP-light responder:

```
Router(config)# ipsla
Router(config-ipsla)# responder twamp-light test-session 1 timeout 100
```

responder twamp light

To configure the TWAMP-light responder, use the **responder twamp-light** command in the **ipsla** configuration mode.

responder twamp-light test-session *test-session-id* [**local-ip** { *local-ip-address* | **any** { **ipv4** | **ipv6** } } **local-port** *local-port-number* **remote-ip** { *remote-ip-address* | **any** { **ipv4** | **ipv6** } } **remote-port** { *remote-port-number* | **any** } **vrf** { *vrf-name* | **any** | **default** } | **timeout** *timeout-value*]

Syntax Description

test-session *test-session-id*	Configure TWAMP-light test-session id. Range: 1 - 65535
local-ip { *local-ip-address* | **any** { **ipv4** | **ipv6** } }	Configure the local ip-address or allow any local IPv4 or IPv6 address
local-port *local-port-number*	Configure the local UDP port number. Range: 1 - 65535
remote-ip { *remote-ip-address* | **any** { **ipv4** | **ipv6** } }	Configure the remote client's ip-address or allow connection from any remote IPv4 or IPv6 address
remote-port { *remote-port-number* | **any** }	Configure the UDP port number of the remote client or allow connection from any remote port. Range: 1 - 65535

vrf { *vrf-name* | **any** | **default** }	Configure vrf for the local ip-address. Possible values for vrf: • *vrf-name* of the vrf of the local ip-address • any: use this only when **local-ip** is configured as any • default: use this when the local ip-address belongs to default vrf
timeout *timeout-value*	Configure the inactivity timeout period (in seconds) For TWAMP-light, the range is 60 - 86400

Command Default

Default timeout is 900 seconds.

Command Modes

IPSLA configuration mode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

- Caution must be taken by the administrator when using **any** option as this configuration opens up the specified **local-port** for packets from any IP address.
- Configure **vrf** as **any** only when you configure **local-ip** as **any**.
- Configure **vrf** with a valid vrf value, when you configure **local-ip** with a valid IPv4/IPv6 address.

Task ID

Task ID	Operation
monitor	read, write

Example

This example shows how to configure the twamp-light responder:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# responder twamp-light test-session 1 local-ip 192.0.2.10 local-port
13001 remote-ip 192.0.2.186 remote-port 13002 vrf default
Router(config-ipsla)# responder twamp-light test-session 1 timeout 60
Router(config-ipsla)# commit
```

samples

To set the number of hop entries that are kept in the history table for an IP SLA ICMP path-echo operation, use the **samples** command in IP SLA operation ICMP path-echo history configuration mode. To use the default value, use the **no** form of this command.

samples *sample-count*
no samples

Syntax Description

sample-count	Number of history samples that are kept in the history table for an IP SLA ICMP path-echo operation. Range is 1 to 30.

Command Default

The default value is 16.

Command Modes

IP SLA operation ICMP path-echo history configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **samples** command is supported only when you configure an IP SLA ICMP path-echo operation.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **samples** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type icmp path-echo
Router(config-ipsla-icmp-path-echo)# history
Router(config-ipsla-op-hist)# samples 30
```

scan delete-factor

To specify the frequency with which the MPLS LSP monitor (MPLSLM) instance searches for provider edge (PE) routers to delete, use the **scan delete-factor** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

scan delete-factor *factor-value*
no scan delete-factor

Syntax Description

factor-value	Specifies a factor that is multiplied by the scan interval to determine the frequency at which the MPLS LSP monitor instance deletes the provider edge (PE) routers that are no longer valid. Range is 0 to 2147483647.

Command Default

factor-value: 1

Command Modes

IP SLA MPLS LSP monitor ping configuration

IP SLA MPLS LSP monitor trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **scan delete-factor** command specifies a factor value for automatic PE deletion. The specified *factor-value* is multiplied by the scan interval to acquire the frequency at which the MPLS LSP monitoring instance deletes not-found PEs. A scan delete factor of zero (0) means that provider edge (PE) routers that are no longer valid are never removed.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **scan delete-factor** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# scan delete-factor 214
```

scan interval

To specify the frequency at which the MPLS LSP monitor (MPLSLM) instance checks the scan queue for updates, use the **scan interval** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

scan interval *scan-interval*
no scan interval

Syntax Description

scan-interval	Time interval between provider edge (PE) router updates. Range is 1 to 70560.

Command Default

interval: 240 minutes

Command Modes IP SLA MPLS LSP monitor ping configuration

IP SLA MPLS LSP monitor trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines Use the **scan interval** command to specify a frequency value in minutes at which the MPLS LSP monitoring instance checks the scan queue for PE updates. Updates from PE discovery are not processed immediately, but rather stored in a scan queue for batched processing at periodic intervals, specified by this value.

Task ID

Task ID	Operations
monitor	read, write

Examples The following example shows how to use the **scan** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# scan interval 120
```

schedule monitor

To schedule MPLS LSP monitoring instances, use the **schedule monitor** command in IP SLA LSP monitor configuration mode. To unschedule the monitoring instances, use the **no** form of this command.

schedule monitor *monitor-id*
no schedule monitor [*monitor-id*]

Syntax Description

monitor-id	Number of the monitoring instance to schedule. Range is 1 to 2048.

Command Default No schedule is configured.

Command Modes IP SLA MPLS LSP monitor configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **schedule monitor** command enters IP SLA MPLS LSP monitor schedule configuration mode so that you can set the desired schedule parameters for the MPLS LSP monitor instance. This schedules the running of all operations created for the specified monitor instance.

To remove all configured schedulers, use the **no schedule monitor** command with no *monitor-id* argument.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to access and use the **schedule monitor** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# schedule monitor 1
Router(config-ipsla-mplslm-sched)#
```

schedule operation

To enter schedule configuration mode, use the **schedule operation** command in IP SLA configuration mode. To remove the scheduler, use the **no** form of this command.

schedule operation *operation-number*
no schedule operation *operation-number*

Syntax Description

operation-number	Configuration number or schedule number that is used to schedule an IP SLA operation. Range is 1 to 2048.

Command Default

None

Command Modes

IP SLA configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **schedule operation** command enters the IP SLA schedule configuration mode. You can configure more schedule configuration parameters to schedule the operation. When an operation is scheduled, it continues collecting information until the configured life expires.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **schedule operation** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# schedule operation 1
Router(config-ipsla-sched)#
```

schedule period

To configure the amount of time during which all LSP operations are scheduled to start or run, use the **schedule period** command in IP SLA MPLS LSP monitor schedule configuration mode. To remove the scheduler, use the **no** form of this command.

schedule period *seconds*
no schedule period

Syntax Description

seconds	Amount of time in seconds for which label switched path (LSP) operations are scheduled to run. Range is 1 to 604800.

Command Default

None

Command Modes

IP SLA MPLS LSP monitor schedule configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **schedule period** command to specify the amount of time in seconds during which all LSP operations are scheduled to start running. All LSP operations are scheduled equally spaced throughout the schedule period.

For example, if the schedule period is 600 seconds and there are 60 operations to be scheduled, they are scheduled at 10-second intervals.

Use the **frequency** command to specify how often the entire set of operations is performed. The frequency value must be greater than or equal to the schedule period.

You must configure the schedule period before you can start MPLS LSP monitoring. Start MPLS LSP monitoring using the **start-time** command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **schedule period** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# schedule monitor 20
Router(config-ipsla-mplslm-sched)# schedule period 6000
```

show ipsla application

To display the information for the IP SLA application, use the **show ipsla application** command in XR EXEC mode.

show ipsla application

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes XR EXEC mode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read

Examples The following sample output is from the **show ipsla application** command:

```
Router# show ipsla application

Estimated system max number of entries: 2048
Number of Entries configured: 1
Number of active Entries    : 0
Number of pending Entries   : 0
Number of inactive Entries  : 1

Supported Operation Types: 7

        Type of Operation: ICMP ECHO
        Type of Operation: ICMP PATH JITTER
        Type of Operation: ICMP PATH ECHO
        Type of Operation: UDP JITTER
        Type of Operation: UDP ECHO
        Type of Operation: MPLS LSP PING
        Type of Operation: MPLS LSP TRACE

Number of configurable probes : 2047
```

```
SA Agent low memory water mark: 20480 (KB)
```

This table describes the significant fields shown in the display.

Table 2: show ipsla application Field Descriptions

Field	Description
Estimated system max number of entries	Maximum number of operations that are configured in the system. The low-memory configured parameter and the available memory in the system are given.
Number of Entries configured	Total number of entries that are configured, such as active state, pending state, and inactive state.
Number of active Entries	Number of entries that are in the active state. The active entries are scheduled and have already started a life period.
Number of pending Entries	Number of entries that are in pending state. The pending entries have a start-time scheduled in the future. These entries either have not started the first life, or the entries are configured as recurring and completed one of its life.
Number of inactive Entries	Number of entries that are in the inactive state. The inactive entries do not have a start-time scheduled. Either the start-time has never been scheduled or life has expired. In addition, the entries are not configured as recurring.
Supported Operation Types	Types of operations that are supported by the system.
Number of configurable probes	Number of remaining entries that can be configured. The number is just an estimated value and it may vary over time according to the available resources.
SA Agent low memory water mark	Available memory for the minimum system below which the IP SLA feature does not configure any more operations.

show ipsla history

To display the history collected for all IP SLA operations or for a specified operation, use the **show ipsla history** command in XR EXEC mode.

show ipsla history [*operation-number*]

Syntax Description

operation-number	(Optional) Number of the IP SLA operation.

Command Default None

Command Modes XR EXEC mode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

By default, history statistics are not collected. To have any data displayed by using the **show ipsla history** command, you must configure the history collection.

This table lists the response return values that are used in the **show ipsla history** command.

Table 3: Response Return Values for the show ipsla history Command

Code	Description
1	Okay
2	Disconnected
3	Over Threshold
4	Timeout
5	Busy
6	Not Connected
7	Dropped
8	Sequence Error
9	Verify Error
10	Application Specific

If the default tabular format is used, the response return description is displayed as code in the Sense column. The Sense field is always used as a return code.

Task ID

Task ID	Operations
monitor	read

Examples

The following sample output is from the **show ipsla history** command:

```
Router# show ipsla history 1

Point by point History
Multiple Lines per Entry
Line 1:
Entry    = Entry number
LifeI    = Life index
BucketI  = Bucket index
SampleI  = Sample index
SampleT  = Sample start time
CompT    = RTT (milliseconds)
```

```
Sense   = Response return code
Line 2 has the Target Address
Entry LifeI       BucketI    SampleI    SampleT        CompT       Sense      TargetAddr
1     0           0          0          1134419252539  9           1          192.0.2.6
1     0           1          0          1134419312509  6           1          192.0.2.6
1     0           2          0          1134419372510  6           1          192.0.2.6
1     0           3          0          1134419432510  5           1          192.0.2.6
```

This table describes the significant fields shown in the display.

Table 4: show ipsla history Field Descriptions

Field	Description
Entry number	Entry number.
LifeI	Life index.
BucketI	Bucket index.
SampleI	Sample index.
SampleT	Sample start time.
CompT	Completion time in milliseconds.
Sense	Response return code.
TargetAddr	IP address of intermediate hop device or destination device.

show ipsla mpls discovery vpn

To display routing information relating to the BGP next-hop discovery database in the MPLS VPN network, use the **show ipsla mpls discovery vpn** command in XR EXEC mode.

show ipsla mpls discovery vpn

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read

Examples

The following sample output is from the **show ipsla mpls discovery vpn** command:

```
Router# show ipsla mpls discovery vpn

Next refresh after: 46 seconds

BGP next hop    Prefix            VRF                             PfxCount
192.255.0.4     192.255.0.4/32    red                             10
                                  blue                            5
                                  green                           7
192.255.0.5     192.255.0.5/32    red                             5
                                  green                           3
192.254.1.6     192.254.1.0/24    yellow                          4
```

This table describes the significant fields shown in the display.

Table 5: show ipsla mpls discovery vpn Field Descriptions

Field	Description
BGP next hop	Identifier for the BGP next-hop neighbor.
Prefix	IPv4 Forward Equivalence Class (FEC) of the BGP next-hop neighbor to be used by the MPLS LSP ping or trace operation.
VRF	Names of the virtual routing and forwarding instances (VRFs) that contain routing entries for the specified BGP next-hop neighbor.
PfxCount	Count of the routing entries that participate in the VRF for the specified BGP next-hop neighbor.

show ipsla mpls lsp-monitor lpd

To display LSP Path Discovery (LPD) operational status, use the **show ipsla mpls lsp-monitor lpd** command in XR EXEC mode.

show ipsla mpls lsp-monitor lpd { **statistics** [*group-ID* | **aggregated** *group-ID*] | **summary** *group* }

statistics *group-ID*	Displays statistics for the specified LPD group, including the latest LPD start time, return code, completion time, and paths.
aggregated *group-ID*	Displays the aggregated statistics of the LPD group.

summary *group- ID*	Displays the current LPD operational status, which includes LPD start time, return code, completion time, and all ECMP path information.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

For the aggregated group ID, a maximum of two buckets are allowed.

Task ID

Task ID	Operations
monitor	read

Examples

The following sample output is from the **show ipsla mpls lsp-monitor lpd statistics** command:

```
Router# show ipsla mpls lsp-monitor lpd statistics 10001

Group ID: 100001
  Latest path discovery start time          : 00:41:01.129 UTC Sat Dec 10 2005
  Latest path discovery return code         : OK
  Latest path discovery completion time (ms): 3450
  Completion Time Values:
    NumOfCompT: 1      CompTMin: 3450    CompTMax : 3450    CompTAvg: 3450
  Number of Paths Values:
    NumOfPaths: 10   MinNumOfPaths: 10   MaxNumOfPaths: 10
```

This table describes the significant fields shown in the display.

Table 6: show ipsla mpls lsp-monitor lpd statistics Field Descriptions

Field	Description
Group ID	LPD group ID number.
Latest path discovery start time	LPD start time.
Latest path discovery return code	LPD return code.
Latest path discovery completion time	LPD completion time.
Completion Time Values	Completion time values, consisting of Number of Completion Time samples and Minimum Completion Time.
Number of Paths Values	Number of paths values, consisting of Minimum number of paths and Maximum number of paths.

show ipsla mpls lsp-monitor scan-queue

To display information about BGP next-hop addresses that are waiting to be added to or deleted from the MPLS label switched path (LSP) monitor instance, use the **show ipsla mpls lsp-monitor scan-queue** command in XR EXEC mode.

show ipsla mpls lsp-monitor scan-queue [*monitor-id*]

Syntax Description

monitor-id	(Optional) Number of the IP SLA MPLS LSP monitor instance.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

If the *monitor-id* argument is not specified, the scan-queue is displayed for all MPLS LSP monitor instances.

Task ID

Task ID	Operations
monitor	read

Examples

The following sample output is from the **show ipsla mpls lsp-monitor scan-queue** command:

```
Router# show ipsla mpls lsp-monitor scan-queue 1

IPSLA MPLS LSP Monitor : 1

  Next scan Time after       : 23 seconds
  Next Delete scan Time after: 83 seconds

  BGP Next hop    Prefix             Add/Delete?
  192.255.0.2     192.255.0.2/32     Add
  192.255.0.3     192.255.0.5/32     Delete
```

This table describes the significant fields shown in the display.

Table 7: show ipsla responder statistics port Field Descriptions

Field	Description
IPSLA MPLS LSP Monitor	Monitor identifier.
Next scan Time after	Amount of time before the MPLS LSP monitor instance checks the scan queue for adding BGP next-hop neighbors. At the start of each scan time, IP SLA operations are created for all newly discovered neighbors.

Field	Description
Next delete Time after	Amount of time left before the MPLS LSP monitor instance checks the scan queue for deleting BGP next-hop neighbors. At the start of each delete scan time, IP SLAs operations are deleted for neighbors that are no longer valid.
BGP next hop	Identifier for the BGP next-hop neighbor.
Prefix	IPv4 Forward Equivalence Class (FEC) of the BGP next-hop neighbor to be used.
Add/Delete	Indicates that the specified BGP next-hop neighbor will be added or removed.

show ipsla mpls lsp-monitor summary

To display the list of operations that have been created automatically by the specified MPLS LSP monitor (MPLSLM) instance, use the **show ipsla mpls lsp-monitor summary** command in XR EXEC mod.

show ipsla mpls lsp-monitor summary [*monitor-id* [**group** [*group id*]]]

Syntax Description

monitor-id	(Optional) Displays a list of LSP group, ping, and trace operations created automatically by the specified MPLSLM instance.
group *group-id*	(Optional) Displays the ECMP LSPs found through ECMP path discovery within the specified LSP group.

Command Default

None

Command Modes

XR EXEC mod

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **show ipsla mpls lsp-monitor summary** command shows the list of LSP operations that were created automatically by the specified MPLS LSP monitor instance. It also shows the current status and the latest operation time of each operation.

If the *monitor-id* argument is not specified, the list of operations is displayed for all MPLS LSP monitor instances.

The **show ipsla mpls lsp-monitor summary** command with the **group** option shows the list of ECMP paths that are found automatically by the specified LSP path discovery (LPD). In addition, this command with option shows the current status; the number of successes, failures; the most recent round trip time (RTT); and the latest operation time of each path.

If the *group-id* argument is not specified, the list of paths is displayed for all operations created by the MPLS LSP monitor instance.

Task ID

Task ID	Operations
monitor	read

Examples

The following sample output is from the **show ipsla mpls lsp-monitor summary** command. This output shows a pending status when an MPLS LSP ping operation is waiting to receive the timeout response from the LSP Verification (LSPV) process.

```
Router# show ipsla mpls lsp-monitor summary 1

MonID  Op/GrpID TargetAddress      Status  Latest Operation Time
1      100001   192.255.0.4/32     up      19:33:37.915 EST Mon Feb 28 2005
1      100002   192.255.0.5/32     down    19:33:47.915 EST Mon Feb 28 2005
1      100003   192.255.0.6/32     pending 19:33:35.915 EST Mon Feb 28 2005
```

The following sample output shows that a down status is displayed after a timeout response is received.

```
Router# show ipsla mpls lsp-monitor summary 1

MonID  Op/GrpID TargetAddress      Status  Latest Operation Time
1      100001   193.100.0.1/32     down    12:47:16.417 PST Tue Oct 23 2007
1      100002   193.100.0.2/32     partial 12:47:22.418 PST Tue Oct 23 2007
1      100003   193.100.0.3/32     partial 12:47:22.429 PST Tue Oct 23 2007
1      100004   193.100.0.4/32     down    12:47:16.429 PST Tue Oct 23 2007
1      100005   193.100.0.5/32     down    12:47:21.428 PST Tue Oct 23 2007
```

This table describes the significant fields shown in the display.

Table 8: show ipsla mpls lsp-monitor summary Field Descriptions

Field	Description
MonID	Monitor identifier.
Op/GrpID	Operation identifiers that have been created by this MPLS LSP monitor instance.
TargetAddress	IPv4 Forward Equivalence Class (FEC) to be used by this operation.
Status	Status of the paths. Values can be as follows: • up—Indicates that the latest operation cycle was successful. • down—Indicates that the latest operation cycle was not successful. • pending—Indicates that the latest operation cycle is waiting for an LSP ping or trace response.
Latest Operation Time	Time the latest operation cycle was issued.

The following sample output is from the **show ipsla mpls lsp-monitor summary group** command:

```
Router# show ipsla mpls lsp-monitor summary 1 group 100001

GrpID  LSP-Selector    Status Failure Success RTT   Latest Operation Time
100001 127.0.0.13      up     0       78      32    20:11:37.895 EST Feb 28 2005
100001 127.0.0.15      retry  1       77      0     20:11:37.995 EST Feb 28 2005
```

```
100001 127.0.0.16      up     0       78      32    20:11:38.067 EST Feb 28 2005
100001 127.0.0.26      up     0       78      32    20:11:38.175 EST Feb 28 2005
```

This table describes the significant fields shown in the display.

Table 9: show ipsla mpls lsp-monitor summary group Field Descriptions

Field	Description
GrpID	Group identifer that has been created by this MPLS LSP monitor instance.
LSP-Selector	LSP selector address.
Status	Status of the paths. Values can be as follows: • up—Indicates that all the paths were successful. • down—Indicates that all the paths were not successful. • partial—Indicates that only some paths were successful. • unknown—Indicates that some (or all) of the paths did not complete a single LSP echo request so the group status could not be identified.
Failure	Number of failures.
Success	Number of successes.
RTT	Round Trip Time (RTT) in milliseconds of the latest LSP echo request for the path.
Latest Operation Time	Time the latest operation cycle was issued for the path.

show ipsla responder statistics

To display the number of probes that are received or handled by the currently active ports on the responder, use the **show ipsla responder statistics ports** command in XR EXEC mode.

show ipsla responder statistics {**all** | **permanent**} **ports**

Syntax Description

all	Port statistics is displayed for all ports.
permanent	Port statistics is displayed only for permanent ports.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The output of the **show ipsla responder statistics port** command is available only for specific intervals of time in which only nonpermanent ports are being used at the responder. The reason is that the responder closes

the nonpermanent ports after each operation cycle. However, if both permanent and nonpermanent ports are used, the output always contains rows for the permanent ports. The rows for the nonpermanent ports are displayed only if those nonpermanent ports are enabled at the instant the command is issued.

Task ID

Task ID	Operations
monitor	read

Examples

The following sample output is from the **show ipsla responder statistics port** command:

```
Router# show ipsla responder statistics all port

Port Statistics
---------------

Local Address  Port   Port Type   Probes   Drops   CtrlProbes   Discard
172.16.5.1     3001   Permanent   0        0       0
172.16.5.1     10001  Permanent   728160   0       24272
172.16.5.5     8201   Dynamic     12132    0       12135        ON
172.16.5.1     4441   Dynamic     207216   0       3641         ON
```

This table describes the significant fields shown in the display.

Table 10: show ipsla responder statistics port Field Descriptions

Field	Description
Local Address	Local IP address of the responder device used to respond to IPSLA probes.
Port	UDP socket local to the responder device used to respond to IPSLA probes.
Port Type	It could be "permanent" or "dynamic"; depends upon whether a permanent port configuration is done.
Probes	Number of probe packets the responder has received.
Drops	Number of probes dropped.
CtrlProbes	Number of control packets the responder has received.
Discard	If the state is ON, the responder will not respond to probes.

show ipsla statistics

To display the operational data and the latest statistics for the IP SLA operation in tabular format, use the **show ipsla statistics** command in XR EXEC mode.

show ipsla statistics [*operation-number*]

Syntax Description

operation-number	(Optional) Operation for which the latest statistics are to be displayed. Range is 1 to 2048.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read

Examples

The output of the **show ipsla statistics** command varies depending on the operation type.

The following sample output is from the **show ipsla statistics** command for an ICMP echo operation:

```
Router# show ipsla statistics 100025

Entry number: 100025
    Modification time: 00:36:58.602 UTC Sat Dec 10 2007
    Start time       : 00:36:58.605 UTC Sat Dec 10 2007
    Number of operations attempted: 5
    Number of operations skipped  : 0
    Current seconds left in Life  : Forever
    Operational state of entry    : Active
    Connection loss occurred      : FALSE
    Timeout occurred              : FALSE
    Latest RTT (milliseconds)     : 3
    Latest operation start time   : 00:41:01.129 UTC Sat Dec 10 2007
    Latest operation return code  : OK
    RTT Values:
      RTTAvg  : 71         RTTMin: 71         RTTMax : 71
      NumOfRTT: 1          RTTSum: 71         RTTSum2: 729
    Path Information:
      Path Path  LSP             Outgoing       Nexthop       Downstream
      Idx  Sense Selector        Interface      Address         Label Stack
      1    1     127.0.0.13      PO0/2/5/0      192.12.1.2      38
      2    1     127.0.0.6       PO0/2/5/0      192.12.1.2      38
      3    1     127.0.0.1       PO0/2/5/0      192.12.1.2      38
      4    1     127.0.0.2       PO0/2/5/0      192.12.1.2      38
      5    1     127.0.0.13      PO0/2/5/1      192.12.2.2      38
      6    1     127.0.0.6       PO0/2/5/1      192.12.2.2      38
      7    1     127.0.0.1       PO0/2/5/1      192.12.2.2      38
      8    1     127.0.0.2       PO0/2/5/1      192.12.2.2      38
      9    1     127.0.0.4       Gi0/2/0/0      192.15.1.2      38
      10   1     127.0.0.5       Gi0/2/0/0      192.15.1.2      38
```

This table describes the significant fields shown in the display.

Table 11: show ipsla statistics Field Descriptions

Field	Description
Entry number	Entry number.
Modification time	Latest time the operation was modified.
Start time	Time the operation was started.
Number of operations attempted	Number of operation cycles that were issued.
Number of operations skipped	Number of operation cycles that were not issued because one of the cycles extended over the configured time interval.
Current seconds left in Life	Time remaining until the operation stops execution.
Operational state of entry	State of the operation, such as active state, pending state, or inactive state.
Connection loss occurred	Whether or not a connection-loss error happened.
Timeout occurred	Whether or not a timeout error happened.
Latest RTT (milliseconds)	Value of the latest RTT sample.
Latest operation start time	Time the latest operation cycle was issued.
Latest operation return code	Return code of the latest operation cycle
RTTAvg	Average RTT value that is observed in the last cycle.
RTTMin	Minimum RTT value that is observed in the last cycle.
RTTMax	Maximum RTT value that is observed in the last cycle.
NumOfRTT	Number of successful round trips.
RTTSum	Sum of all successful round-trip values in milliseconds.
RTTSum2	Sum of squares of the round-trip values in milliseconds.
Path Idx	Path index number.
Path Sense	Response return code for the path.
LSP Selector	LSP selector address of the path.
Outgoing Interface	Outgoing interface of the path.
Nexthop Address	Next hop address of the path.
Downstream Label Stack	MPLS label stacks of the path.

show ipsla statistics aggregated

To display the hourly statistics for all the IP SLA operations or specified operation, use the **show ipsla statistics aggregated** command in XR EXEC mode.

show ipsla statistics aggregated [**detail**] [*operation-number*]

Syntax Description

detail	Displays detailed information.
operation-number	(Optional) Number of IP SLA operations. Range is 1 to 2048.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **show ipsla statistics aggregated** command displays information such as the number of failed operations and the reason for failure. Unless you configured a different amount of time for the **buckets** command (**statistics** command with **hourly** keyword), the **show ipsla statistics aggregated** command displays the information collected over the past two hours.

For one-way delay and jitter operations to be computed for UDP jitter operations, the clocks on local and target devices must be synchronized using NTP or GPS systems. If the clocks are not synchronized, one-way measurements are discarded. If the sum of the source to destination (SD) and the destination to source (DS) values is not within 10 percent of the round-trip time, the one-way measurement values are assumed to be faulty, and are discarded.

Task ID

Task ID	Operations
monitor	read

Examples

The output of the **show ipsla statistics aggregated** command varies depending on operation type. The following sample output shows the aggregated statistics for UDP echo operation from the **show ipsla statistics aggregated** command:

```
Router# show ipsla statistics aggregated 1

Entry number: 1
Hour Index: 0
    Start Time Index: 21:02:32.510 UTC Mon Dec 12 2005
    Number of Failed Operations due to a Disconnect     : 0
    Number of Failed Operations due to a Timeout        : 0
    Number of Failed Operations due to a Busy           : 0
    Number of Failed Operations due to a No Connection  : 0
    Number of Failed Operations due to an Internal Error: 0
```

```
    Number of Failed Operations due to a Sequence Error : 0
    Number of Failed Operations due to a Verify Error   : 0
    RTT Values:
      RTTAvg  : 6          RTTMin: 4          RTTMax : 38
      NumOfRTT: 36         RTTSum: 229        RTTSum2: 2563
```

The following sample output is from the **show ipsla statistics aggregated** command in which operation 10 is a UDP jitter operation:

```
Router# show ipsla statistics aggregated 10

Entry number: 10
Hour Index: 0
    Start Time Index: 00:35:07.895 UTC Thu Mar 16 2006
    Number of Failed Operations due to a Disconnect     : 0
    Number of Failed Operations due to a Timeout        : 0
    Number of Failed Operations due to a Busy           : 0
    Number of Failed Operations due to a No Connection  : 0
    Number of Failed Operations due to an Internal Error: 0
    Number of Failed Operations due to a Sequence Error : 0
    Number of Failed Operations due to a Verify Error   : 0
    RTT Values:
      RTTAvg  : 14         RTTMin: 2          RTTMax : 99
      NumOfRTT: 70         RTTSum: 1034       RTTSum2: 60610
    Packet Loss Values:
      PacketLossSD       : 0          PacketLossDS: 0
      PacketOutOfSequence: 0          PacketMIA   : 0
      PacketLateArrival  : 0
      Errors             : 0          Busies      : 0
    Jitter Values :
      MinOfPositivesSD: 1          MaxOfPositivesSD: 19
      NumOfPositivesSD: 17         SumOfPositivesSD: 65
      Sum2PositivesSD : 629
      MinOfNegativesSD: 1          MaxOfNegativesSD: 16
      NumOfNegativesSD: 24         SumOfNegativesSD: 106
      Sum2NegativesSD : 914
      MinOfPositivesDS: 1          MaxOfPositivesDS: 7
      NumOfPositivesDS: 17         SumOfPositivesDS: 44
      Sum2PositivesDS : 174
      MinOfNegativesDS: 1          MaxOfNegativesDS: 8
      NumOfNegativesDS: 24         SumOfNegativesDS: 63
      Sum2NegativesDS : 267
      Interarrival jitterout: 0              Interarrival jitterin: 0
    One Way Values :
      NumOfOW: 0
      OWMinSD : 0          OWMaxSD: 0          OWSumSD: 0
      OWSum2SD: 0
      OWMinDS : 0          OWMaxDS: 0          OWSumDS: 0
```

This table describes the significant fields shown in the display.

Table 12: show ipsla statistics aggregated Field Descriptions

Field	Description
Busies	Number of times that the operation cannot be started because the previously scheduled run was not finished.
Entry Number	Entry number.
Hop in Path Index	Hop in path index.

Field	Description
Errors	Number of internal errors.
Jitter Values	Jitter statistics appear on the specified lines. Jitter is defined as interpacket delay variance.
NumOfJitterSamples	Number of jitter samples that are collected. The number of samples are used to calculate the jitter statistics.
Number of Failed Operations due to a Disconnect	Number of failed operations due to a disconnect.
Number of Failed Operations due to a Timeout	Number of failed operations due to a timeout.
Number of Failed Operations due to a Busy	Number of failed operations due to a busy error.
Number of Failed Operations due to a No Connection	Error that refers to the case in which the control connection cannot be established.
Number of Failed Operations due to an Internal Error	Number of failed operations due to an internal error.
Number of Failed Operations due to a Sequence Error	Number of failed operations due to a sequence error.
Number of Failed Operations due to a Verify Error	Number of failed operations due to a verify error.
MaxOfNegativesSD	Maximum negative jitter values from the source to the destination. The absolute value is given.
MaxOfPositivesSD	Maximum jitter values from the source to the destination in milliseconds.
MaxOfPositivesDS	Maximum jitter values from the destination to the source in milliseconds.
MaxOfNegativesDS	Maximum negative jitter values from destination-to-source. The absolute value is given.
MinOfPositivesDS	Minimum jitter values from the destination to the source in milliseconds.
MinOfNegativesSD	Minimum negative jitter values from the source to the destination. The absolute value is given.
MinOfPositivesSD	Minimum jitter values from the source to the destination in milliseconds.
MinOfNegativesDS	Minimum negative jitter values from the destination to the source. The absolute value is given.

Field	Description
NumOfOW	Number of successful one-way time measurements.
NumOfNegativesDS	Number of jitter values from the destination to the source that are negative; for example, network latency decreases for two consecutive test packets.
NumOfNegativesSD	Number of jitter values from the source to the destination that are negative; for example, network latency decreases for two consecutive test packets.
NumOfPositivesDS	Number of jitter values from the destination to the source that are positive; for example, network latency increases for two consecutive test packets.
NumOfPositivesSD	Number of jitter values from the source to the destination that are positive; for example, network latency increases for two consecutive test packets.
NumOfRTT	Number of successful round trips.
One Way Values	One-way measurement statistics appear on the specified lines. One Way (OW) values are the amount of time that it took the packet to travel from the source router to the target router or from the target router to the source router.
OWMaxDS	Maximum time from the destination to the source.
OWMaxSD	Maximum time from the source to the destination.
OWMinDS	Minimum time from the destination to the source.
OWMinSD	Minimum time from the source to the destination.
OWSumDS	Sum of one-way delay values from the destination to the source.
OWSumSD	Sum of one-way delay values from the source to the destination.
OWSum2DS	Sum of squares of one-way delay values from the destination to the source.
OWSum2SD	Sum of squares of one-way delay values from the source to the destination.
PacketLateArrival	Number of packets that arrived after the timeout.
PacketLossDS	Number of packets lost from the destination to the source (DS).
PacketLossSD	Number of packets lost from the source to the destination (SD).
PacketMIA	Number of packets lost in which the SD direction or DS direction cannot be determined.
PacketOutOfSequence	Number of packets that are returned out of order.

Field	Description
Path Index	Path index.
Port Number	Target port number.
RTTSum	Sum of all successful round-trip values in milliseconds.
RTTSum2	Sum of squares of the round-trip values in milliseconds.
RTT Values	Round-trip time statistics appear on the specified lines.
Start Time	Start time, in milliseconds.
Start Time Index	Statistics that are aggregated for over 1-hour intervals. The value indicates the start time for the 1-hour interval that is displayed.
SumOfPositivesDS	Sum of the positive jitter values from the destination to the source.
SumOfPositivesSD	Sum of the positive jitter values from the source to the destination.
SumOfNegativesDS	Sum of the negative jitter values from the destination to the source.
SumOfNegativesSD	Sum of the negative jitter values from the source to the destination.
Sum2PositivesDS	Sum of squares of the positive jitter values from the destination to the source.
Sum2PositivesSD	Sum of squares of the positive jitter values from the source to the destination.
Sum2NegativesDS	Sum of squares of the negative jitter values from the destination to the source.
Sum2NegativesSD	Sum of squares of the negative jitter values from the source to the destination.
Target Address	Target IP address.

The output of the **show ipsla statistics aggregated detail** command varies depending on operation type. The following sample output is from the **show ipsla statistics aggregated detail** command in tabular format, when the output is split over multiple lines:

```
Router# show ipsla statistics aggregated detail 2

Captured Statistics
        Multiple Lines per Entry
Line1:
Entry    = Entry number
StartT   = Start time of entry (hundredths of seconds)
Pth      = Path index
Hop      = Hop in path index
Dst      = Time distribution index
Comps    = Operations completed
SumCmp   = Sum of RTT (milliseconds)

Line2:
```

```
SumCmp2H = Sum of RTT squared high 32 bits (milliseconds)
SumCmp2L = Sum of RTT squared low 32 bits (milliseconds)
TMax     = RTT maximum (milliseconds)
TMin     = RTT minimum (milliseconds)

Entry StartT         Pth Hop Dst Comps      SumCmp
      SumCmp2H       SumCmp2L    TMax       TMin
2     1134423910701 1   1   0   12         367
      0              1231        6          6
2     1134423851116 1   1   1   2          129
      0              2419        41         41
2     1134423070733 1   1   2   1          101
      0              1119        16         16
2     0              1   1   3   0          0
      0              0           0          0
```

This table describes the significant fields shown in the display.

Table 13: show ipsla statistics aggregated detail Field Descriptions

Field	Description
Entry	Entry number.
StartT	Start time of entry, in hundredths of seconds.
Pth	Path index.
Hop	Hop in path index.
Dst	Time distribution index.
Comps	Operations completed.
SumCmp	Sum of completion times, in milliseconds.
SumCmp2L	Sum of completion times squared low 32 bits, in milliseconds.
SumCmp2H	Sum of completion times squared high 32 bits, in milliseconds.
TMax	Completion time maximum, in milliseconds.
TMin	Completion time minimum, in milliseconds.

The following sample output is from the **show ipsla statistics aggregated** command when a path discovery operation is enabled. Data following the hourly index is aggregated for all paths in the group during the given hourly interval.

```
Router# show ipsla statistics aggregated 100041

Entry number: 100041

Hour Index: 13

<The following data after the given hourly index is aggregated for all paths in the group
during the given hourly interval.>

    Start Time Index: 12:20:57.323 UTC Tue Nov 27 2007
    Number of Failed Operations due to a Disconnect     : 0
```

```
    Number of Failed Operations due to a Timeout        : 249
    Number of Failed Operations due to a Busy           : 0
    Number of Failed Operations due to a No Connection  : 0
    Number of Failed Operations due to an Internal Error: 0
    Number of Failed Operations due to a Sequence Error : 0
    Number of Failed Operations due to a Verify Error   : 0
<end>
    RTT Values:
      RTTAvg  : 21         RTTMin: 19         RTTMax : 73
      NumOfRTT: 2780       RTTSum: 59191      RTTSum2: 1290993

<The following data for LSP path information is available after path discovery is enabled.>


    Path Information:
      Path Path  LSP             Outgoing        Nexthop         Downstream
      Idx  Sense Selector        Interface       Address         Label Stack
      1    1     127.0.0.1       Gi0/4/0/0       192.39.1.1      677
      2    1     127.0.0.1       Gi0/4/0/0.1     192.39.2.1      677
      3    1     127.0.0.1       Gi0/4/0/0.2     192.39.3.1      677
      4    1     127.0.0.1       Gi0/4/0/0.3     192.39.4.1      677
      5    1     127.0.0.8       Gi0/4/0/0       192.39.1.1      677
      6    1     127.0.0.8       Gi0/4/0/0.1     192.39.2.1      677
      7    1     127.0.0.8       Gi0/4/0/0.2     192.39.3.1      677
      8    1     127.0.0.8       Gi0/4/0/0.3     192.39.4.1      677
<end>
Hour Index: 14
    Start Time Index: 13:20:57.323 UTC Tue Nov 27 2007
    Number of Failed Operations due to a Disconnect     : 0
    Number of Failed Operations due to a Timeout        : 122
    Number of Failed Operations due to a Busy           : 0
    Number of Failed Operations due to a No Connection  : 0
    Number of Failed Operations due to an Internal Error: 0
    Number of Failed Operations due to a Sequence Error : 0
    Number of Failed Operations due to a Verify Error   : 0
    RTT Values:
      RTTAvg  : 21         RTTMin: 19         RTTMax : 212
      NumOfRTT: 3059       RTTSum: 65272      RTTSum2: 1457612
    Path Information:
      Path Path  LSP             Outgoing        Nexthop         Downstream
      Idx  Sense Selector        Interface       Address         Label Stack
      1    1     127.0.0.1       Gi0/4/0/0       192.39.1.1      677
      2    1     127.0.0.1       Gi0/4/0/0.1     192.39.2.1      677
      3    1     127.0.0.1       Gi0/4/0/0.2     192.39.3.1      677
      4    1     127.0.0.1       Gi0/4/0/0.3     192.39.4.1      677
      5    1     127.0.0.8       Gi0/4/0/0       192.39.1.1      677
      6    1     127.0.0.8       Gi0/4/0/0.1     192.39.2.1      677
      7    1     127.0.0.8       Gi0/4/0/0.2     192.39.3.1      677
      8    1     127.0.0.8       Gi0/4/0/0.3     192.39.4.1      677
```

This table describes the significant fields shown in the display.

Table 14: show ipsla statistics aggregated (with Path Discovery enabled) Field Descriptions

Field	Description
Entry Number	Entry number.
Start Time Index	Start time.
Number of Failed Operations due to a Disconnect	Number of failed operations due to a disconnect.

Field	Description
Number of Failed Operations due to a Timeout	Number of failed operations due to a timeout.
Number of Failed Operations due to a Busy	Number of failed operations due to a busy error.
Number of Failed Operations due to a No Connection	Error that refers to the case in which the control connection cannot be established.
Number of Failed Operations due to an Internal Error	Number of failed operations due to an internal error.
Number of Failed Operations due to a Sequence Error	Number of failed operations due to a sequence error.
Number of Failed Operations due to a Verify Error	Number of failed operations due to a verify error.
RTT Values	Round-trip time statistics appear on the specified lines.
RTT Min/Avg/Max	Maximum values of the RTT that are observed in the latest cycle (*).
NumOfRTT	Number of successful round trips.
RTT Sum	Sum of all successful round-trip values, in milliseconds.
RTT Sum2	Sum of squares of the round-trip values, in milliseconds.
RTT Min/Avg/Max	Maximum values of the RTT that are observed in the latest cycle (*).
NumOfRTT	Number of successful round trips.
Path Idx	Path index number.
Path Sense	Response return code for the path.
LSP Selector	LSP selector address of the path.
Outgoing Interface	Outgoing interface name of the path.
Nexthop Address	Next hop address of the path.
Downstream Label Stack	MPLS label stacks of the path.

show ipsla statistics enhanced aggregated

To display the enhanced history statistics for all collected enhanced history buckets for the specified IP SLA operation, use the **show ipsla statistics enhanced aggregated** command in XR EXEC mode.

show ipsla statistics enhanced aggregated [*operation-number*] [**interval** *seconds*]

Syntax Description

operation-number	(Optional) Operation number for which to display the enhanced history distribution statistics.
interval *seconds*	(Optional) Specifies the aggregation interval in seconds for which to display the enhanced history distribution statistics.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **show ipsla statistics enhanced aggregated** command displays data for each bucket of enhanced history data shown individually; for example, one after the other. The number of buckets and the collection interval is set using the **interval** keyword, *seconds* argument, **buckets** keyword, and *number-of-buckets* argument.

Task ID

Task ID	Operations
monitor	read

Examples

The output of the **show ipsla statistics enhanced aggregated** command varies depending on the operation type.

The following sample output is from the **show ipsla statistics enhanced aggregated** command for the UDP echo operation:

```
Router# show ipsla statistics enhanced aggregated 20

Entry number: 20
Interval : 300 seconds
  Bucket : 1   (0   - 300 seconds)
    Start Time Index: 00:38:14.286 UTC Thu Mar 16 2006
    Number of Failed Operations due to a Disconnect     : 0
    Number of Failed Operations due to a Timeout        : 0
    Number of Failed Operations due to a Busy           : 0
    Number of Failed Operations due to a No Connection  : 0
    Number of Failed Operations due to an Internal Error: 0
    Number of Failed Operations due to a Sequence Error : 0
    Number of Failed Operations due to a Verify Error   : 0
    RTT Values:
      RTTAvg  : 2          RTTMin: 2          RTTMax : 5
      NumOfRTT: 5          RTTSum: 13         RTTSum2: 41
  Bucket : 2   (300 - 600 seconds)
    Start Time Index: 00:43:12.747 UTC Thu Mar 16 2006
    Number of Failed Operations due to a Disconnect     : 0
    Number of Failed Operations due to a Timeout        : 0
    Number of Failed Operations due to a Busy           : 0
    Number of Failed Operations due to a No Connection  : 0
    Number of Failed Operations due to an Internal Error: 0
    Number of Failed Operations due to a Sequence Error : 0
    Number of Failed Operations due to a Verify Error   : 0
```

```
RTT Values:
  RTTAvg  : 2          RTTMin: 2          RTTMax : 2
  NumOfRTT: 1          RTTSum: 2          RTTSum2: 4
```

This table describes the significant fields shown in the display.

Table 15: show ipsla statistics enhanced aggregated Field Descriptions

Field	Description
Entry Number	Entry number.
Interval	Multiple of the frequency of the operation. The Enhanced interval field defines the interval in which statistics displayed by the **show ipsla statistics enhanced aggregated** command are aggregated. This field must be configured so that the enhanced aggregated statistics are displayed.
Bucket	Bucket index.
Start Time Index	Statistics that are aggregated depend on the interval configuration mode. The value depends on the interval configuration that is displayed.
RTT Values	Round-trip time statistics appear on the specified lines.
RTT Min/Avg/Max	Maximum values of the RTT that are observed in the latest cycle (*).
NumOfRTT	Number of successful round trips.
RTT Sum	Sum of all successful round-trip values, in milliseconds.
RTT Sum2	Sum of squares of the round-trip values, in milliseconds.
Number of Failed Operations due to a Disconnect	Number of failed operations due to a disconnect.
Number of Failed Operations due to a Timeout	Number of failed operations due to a timeout.
Number of Failed Operations due to a Busy	Number of failed operations due to a busy error.
Number of Failed Operations due to a No Connection	Error that refers to the case in which the control connection cannot be established.
Number of Failed Operations due to an Internal Error	Number of failed operations due to an internal error.
Number of Failed Operations due to a Sequence Error	Number of failed operations due to a sequence error.
Number of Failed Operations due to a Verify Error	Number of failed operations due to a verify error.

show ipsla twamp connection

To display the Two-Way Active Management Protocol (TWAMP) connections, use the **show ipsla twamp conection** command in the XR EXEC mode.

show ipsla twamp connection [**detail** *source-ip* | **requests**]

Syntax Description

detail *source-ip*	Displays details of the connection for a specified source-ip.
requests	Displays request details.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
ip-services	read

Example

This example shows how to run the **show ipsla twamp conection** command with the **requests** keyword:

```
Router# show ipsla twamp connection requests
```

source address

To identify the address of the source device, use the **source address** command in the appropriate configuration mode. To use the best local address, use the **no** form of this command.

source address *ipv4-address*
no source address

Syntax Description

ipv4-address	IP address or hostname of the source device.

Command Default

IP SLA finds the best local address to the destination and uses it as the source address.

Command Modes

IP SLA UDP echo configuration

IP SLA UDP jitter configuration

IP SLA ICMP path-jitter configuration

IP SLA ICMP path-echo configuration

IP SLA ICMP echo configuration

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to designate an IP address for the **source address** command in IP SLA UDP jitter configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# source address 192.0.2.9
```

source port

To identify the port of the source device, use the **source port** command in the appropriate configuration mode. To use the unused port number, use the **no** form of this command.

source port *port*
no source port

Syntax Description

port *port*	Identifies the port number of the source device. Range is 1 to 65535.

Command Default

IP SLA uses an unused port that is allocated by system.

Command History

Releas	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **source port** command is not supported to configure ICMP operations; it is supported only to configure UDP operations.

The specified source port should not be used in other IPSLA operations configured on the same source IP address and source VRF.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to designate a port for the **source port** command in IP SLA UDP jitter configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# source port 11111
```

start-time

To determine the time when the operation or MPLS LSP monitor instance starts, use the **start-time** command in the appropriate configuration mode. To stop the operation and place it in the default state, use the **no** form of this command.

start-time { *hh* **:** *mm* **:** *ss* [*day* | *month* *day* *year*] | **after** *hh* **:** *mm* **:** *ss* | **now** | **pending** }
no start-time

Syntax Description

hh:mm:ss	Absolute start time in hours, minutes, and seconds. You can use the 24-hour clock notation. For example, the **start-time** *01:02* is defined as 1:02 am, or **start-time** *13:01:30* is defined as start at 1:01 pm. and 30 seconds. The current day is used; unless, you specify a *month* and *day*.
month	(Optional) Name of the month to start the operation. When you use the *month* argument, you are required to specify a day. You can specify the month by using the full English name or the first three letters of the month.
day	(Optional) Number of the day, in the range of 1 to 31, to start the operation. In addition, you must specify a month.
year	(Optional) Year in the range of 1993 to 2035.
after *hh:mm:ss*	Specifies that the operation starts at *hh* hours, *mm* minutes, and *ss* seconds after the **start-time** command is used.
now	Specifies that the operation should start immediately.
pending	Specifies that no information is collected. The default value is the **pending** keyword.

Command Default

If a month and day are not specified, the current month and day are used.

Command Modes

IP SLA schedule configuration

IP SLA MPLS LSP monitor schedule configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

If the **start-time** command is used in IP SLA operation mode, it configures the start time for the specific operation being configured. If the **start-time** command is used in IP SLA MPLS LSP monitor mode, it configures the start time for all monitor instances associated with the monitored provider edge (PE) routers.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **start-time** command option for the schedule operation:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# schedule operation 1
Router(config-ipsla-sched)# start-time after 01:00:00
```

The following example shows how to use the **start-time** command in IP SLA MPLS LSP monitor schedule configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# schedule monitor 1
Router(config-ipsla-mplslm-sched)# start-time after 01:00:00
```

The following example shows how to use the **start-time** command and specify a year for a scheduled operation:

```
Router# configure
Router(config)# ipsla operation 2
Router(config-ipsla-op)# type icmp echo
Router(config-ipsla-icmp-echo)# destination address 192.0.2.9
Router(config-ipsla-icmp-echo)# exit
Router(config-ipsla-op)# exit
Router(config-ipsla)# schedule operation 2
Router(config-ipsla-sched)# start 20:0:0 february 7 2008
Router(config-ipsla-sched)#
```

statistics

To set the statistics collection parameters for the operation, use the **statistics** command in the appropriate configuration mode. To remove the statistics collection or use the default value, use the **no** form of this command.

statistics { **hourly** | **interval** *seconds* }
no statistics { **hourly** | **interval** *seconds* }

Syntax Description

hourly	Sets the distribution for statistics configuration that is aggregated for over an hour.
interval *seconds*	Collects statistics over a specified time interval. Interval (in seconds) over which to collect statistics. Range is 1 to 3600 seconds.

Command Default

None

Command Modes

IP SLA operation UDP jitter configuration

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

IP SLA MPLS LSP monitor ping configuration

IP SLA MPLS LSP monitor trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **statistics interval** command is not supported for the configuration of ICMP path-echo and ICMP path-jitter operations, nor for the configuration of MPLS LSP monitor instances.

If the **statistics** command is used in IP SLA operation mode, it configures the statistics collection for the specific operation being configured. If the **statistics** command is used in IP SLA MPLS LSP monitor mode, it configures the statistics collection for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to set the number of hours in which statistics are maintained for the IP SLA UDP jitter operation for the **statistics** command:

```
Router# configure
Router(config)# ipsla
```

```
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# statistics hourly
Router(config-ipsla-op-stats)#
```

The following example shows how to collect statistics for a specified time interval, using the **statistics** command in an IP SLA UDP jitter operation:

```
Router# configure
Router(config)# ipsla operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# statistics interval 60
Router(config-ipsla-op-stats)#
```

The following example shows how to set the number of hours in which statistics are maintained for the IP SLA MPLS LSP monitor ping operation, using the **statistics** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# statistics hourly
Router(config-ipsla-mplslm-stats)#
```

tag (IP SLA)

To create a user-specified identifier for an IP SLA operation, use the **tag** command in the appropriate configuration mode. To unset the tag string, use the **no** form of this command.

tag [*text*]
no tag

Syntax Description

text	(Optional) Specifies a string label for the IP SLA operation.

Command Default

No tag string is configured.

Command Modes

IP SLA UDP echo configuration

IP SLA UDP jitter configuration

IP SLA ICMP path-jitter configuration

IP SLA ICMP path-echo configuration

IP SLA ICMP echo configuration

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

IP SLA MPLS LSP monitor ping configuration

IP SLA MPLS LSP monitor trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

If the **tag** command is used in IP SLA operation mode, it configures the user-defined tag string for the specific operation being configured. If the **tag** command is used in IP SLA MPLS LSP monitor mode, it configures the user-defined tag string for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **tag** command in IP SLA UDP jitter configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# tag ipsla
```

The following example shows how to use the **tag** command in IP SLA MPLS LSP monitor ping configuration mode:

```
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 1
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# tag mplslm-tag
```

target ipv4

To specify the IPv4 address of the target router to be used in an MPLS LSP ping or MPLS LSP trace operation, use the **target ipv4** command in the appropriate configuration mode. To unset the address, use the **no** form of this command.

target ipv4 *destination-address destination-mask*
no target ipv4

Syntax Description

destination-address	IPv4 address of the target device to be tested.

destination-mask	Number of bits in the network mask of the target address. The network mask can be specified in either of two ways: • The network mask can be a four-part dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit belongs to the network address. • The network mask can be indicated as a slash (/) and number. For example, /8 indicates that the first 8 bits of the mask are ones, and the corresponding bits of the address are network address.

Command Default

None

Command Modes

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **target ipv4** command to specify the IPv4 address of the target router at the end of the LSP to be tested or traced and to indicate the destination as an Label Distribution Protocol (LDP) IPv4 address. The target IPv4 address identifies the appropriate label stack associated with the LSP.

Note Using the **target ipv4** command, you can configure only one LDP IPv4 address as the target in an MPLS LSP ping or trace operation. If you enter the command a second time and configure a different IPv4 target address, you overwrite the first IPv4 address.

An MPLS LSP ping operation tests connectivity in the LSP using verification on the specified Forwarding Equivalence Class (FEC)— in this case, LDP IPv4 prefix—between the ping origin and the egress node identified with the **target ipv4** command. This test is carried out by sending an MPLS echo request along the same data path as other packets belonging to the FEC. When the ping packet reaches the end of the path, it is sent to the control plane of the egress label switching router (LSR), which then verifies that it is indeed an egress for the LSP. The MPLS echo request contains information about the LSP that is being verified.

In an MPLS network, an MPLS LSP trace operation traces LSP paths to the target router identified with the **target ipv4** command. In the verification of LSP routes, a packet is sent to the control plane of each transit LSR, which performs various checks, including one that determines if it is a transit LSR for the LSP path. Each transit LSR also returns information related to the LSP being tested (that is, the label bound to the LDP IPv4 prefix).

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **target ipv4** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp ping
Router(config-ipsla-mpls-lsp-ping)# target ipv4 192.168.1.4 255.255.255.255
```

target pseudowire

To specify the pseudowire as the target to be used in an MPLS LSP ping operation, use the **target pseudowire** command in IP SLA MPLS LSP ping configuration mode. To unset the target, use the **no** form of this command.

target pseudowire *destination-address circuit-id*
no target pseudowire

Syntax Description

destination-address	IPv4 address of the target device to be tested.
circuit-id	Virtual circuit identifier. Range is 1 to 4294967295.

Command Default

No default behavior or values

Command Modes

IP SLA MPLS LSP ping configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **target pseudowire** command to specify a target router and to indicate the destination as a Layer 2 VPN pseudowire in an MPLS LSP ping operation. The **target pseudowire** command identifies the target address and the virtual circuit (VC) identifier.

Note Using the **target pseudowire** command, you can configure only one pseudowire address as the target in an MPLS LSP ping operation. If you use the command a second time and configure a different pseudowire target address, the first pseudowire address is overwritten.

A pseudowire target of the LSP ping operation allows active monitoring of statistics on Pseudowire Edge-to-Edge (PWE3) services across an MPLS network. PWE3 connectivity verification uses the Virtual Circuit Connectivity Verification (VCCV).

For more information on VCCV, refer to the VCCV draft, “Pseudowire Virtual Circuit Connectivity Verification (VCCV)” on the IETF web page.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **target pseudowire** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp ping
Router(config-ipsla-mpls-lsp-trace)# target pseudowire 192.168.1.4 4211
```

target traffic-eng

To specify the target MPLS traffic engineering tunnel to be used in an MPLS LSP ping or MPLS LSP trace operation, use the **target traffic-eng** command in the appropriate configuration mode. To unset the tunnel, use the **no** form of this command.

target traffic-eng tunnel *tunnel-interface*
no target traffic-eng

Syntax Description

tunnel *tunnel-interface*	Tunnel ID of an MPLS traffic-engineering tunnel (for example, tunnel 10) configured on the router. Range is 0 to 65535.

Command Default

No default behavior or values

Command Modes

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **target traffic-eng** command to specify a target router and to indicate the destination as an MPLS traffic-engineering (TE) tunnel in an MPLS LSP ping or MPLS LSP trace operation. The **target traffic-eng** command identifies the tunnel interface and the appropriate label stack associated with the LSP to be pinged or traced. An LSP tunnel interface is the head-end of a unidirectional virtual link to a tunnel destination.

Note Using the **target traffic-eng** command, you can configure only one MPLS TE tunnel as the target in an MPLS LSP ping or trace operation. If you enter the command a second time and configure a different tunnel interfaces, you overwrite the first tunnel ID.

An IP SLA ping operation tests connectivity in the LSP using verification on the specified Forwarding Equivalence Class (FEC)—in this case, MPLS TE tunnel—between the ping origin and the egress node identified with the **target traffic-eng** command. This test is carried out by sending an MPLS echo request along the same data path as other packets belonging to the tunnel. When the ping packet reaches the end of the path, it is sent to the control plane of the egress label switching router (LSR), which then verifies that it is indeed an egress for the MPLS TE tunnel. The MPLS echo request contains information about the tunnel whose LSP path is being verified.

In an MPLS network, an IP SLA trace operation traces the LSP paths to a target router identified with the **target traffic-eng** command. In the verification of LSP routes, a packet is sent to the control plane of each transit LSR, which performs various checks, including one that determines if it is a transit LSR for the LSP path. Each transit LSR also returns information related to the MPLS TE tunnel to see if the local forwarding information matches what the routing protocols determine as the LSP path.

MPLS traffic engineering automatically establishes and maintains LSPs across the backbone. The path that an LSP uses is determined by the LSP resource requirements and network resources, such as bandwidth.

For more information on MPLS traffic-engineering tunnels, refer to *MPLS Traffic Engineering and Enhancements*.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **target traffic-eng tunnel** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp trace
Router(config-ipsla-mpls-lsp-trace)# target traffic-eng tunnel 101
```

threshold

To set the lower-limit and upper-limit values, use the **threshold** command in IP SLA reaction condition configuration mode. To use the default value, use the **no** form of this command.

threshold lower-limit *value* **upper-limit** *value*
no threshold lower-limit *value* **upper-limit** *value*

Syntax Description

lower-limit *value*	Specifies the threshold lower-limit value. Range is 1 to 4294967295 ms. Default **lower-limit** value is 3000 ms.
upper-limit *value*	Specifies the threshold upper-limit value. Range is 5000 to 4294967295 ms. Default **upper-limit** value is 5000 ms.

Command Default

lower-limit *value*: 3000 ms

upper-limit *value*: 5000 ms

Command Modes

IP SLA reaction condition configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **threshold** command is supported only when used with the **react** command and **jitter-average** and **packet-loss** keywords.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to set the lower-limit and upper-limit values for the **react** command with the **jitter-average** keyword for the **threshold** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react jitter-average
Router(config-ipsla-react-cond)# threshold lower-limit 8000 upper-limit 10000
```

The following example shows how to set the lower-limit and upper-limit values for the **react** command with the **packet-loss** keyword for the **threshold** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react packet-loss dest-to-source
Router(config-ipsla-react-cond)# threshold lower-limit 8000 upper-limit 10000
```

threshold type average

To take action on average values to violate a threshold, use the **threshold type average** command in IP SLA reaction condition configuration mode. To clear the threshold type (reaction will never happen), use the **no** form of this command.

threshold type average *number-of-probes*
no threshold type

Syntax Description

number-of-probes	When the average of the last five values for the monitored element exceeds the upper threshold or the average of the last five values for the monitored element drops below the lower threshold, the action is performed as defined by the **action** command. Range is 1 to 16.

Command Default

If there is no default value, no threshold type is configured.

Command Modes

IP SLA reaction condition configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **threshold type average** command is supported only when used with the **react** command and **jitter-average**, **packet-loss**, and **rtt** keywords.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to set the number of probes for the **react** command with the **jitter-average** keyword for the **threshold type average** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react jitter-average
Router(config-ipsla-react-cond)# threshold type average 8
```

The following example shows how to set the number of probes for the **react** command with the **packet-loss** keyword for the **threshold type average** command:

```
Router# configure
Router(config)# ipsla reaction operation 432
Router(config-ipsla-react)# react packet-loss dest-to-source
Router(config-ipsla-react-cond)# threshold type average 8
```

threshold type consecutive

To take action after a number of consecutive violations, use the **threshold type consecutive** command in the appropriate configuration mode. To clear the threshold type (reaction will never happen), use the **no** form of this command.

threshold type consecutive *occurrences*
no threshold type

Syntax Description

occurrences	When the reaction condition is set for a consecutive number of occurrences, there is no default value. The number of occurrences is set when specifying the threshold type. The number of consecutive violations is 1 to 16.

Command Default

No default behavior or values

Command Modes

IP SLA reaction condition configuration

IP SLA MPLS LSP monitor reaction condition configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

If the **threshold type consecutive** command is used in IP SLA reaction condition mode, it configures the threshold for the specific operation being configured. If the **threshold type consecutive** command is used in IP SLA MPLS LSP monitor reaction condition configuration mode, it configures the threshold for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **threshold type consecutive** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react jitter-average
Router(config-ipsla-react-cond)# threshold type consecutive 8
```

The following example shows how to use the **threshold type consecutive** command in IP SLA MPLS LSP monitor reaction condition configuration mode:

```
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# reaction monitor 2
Router(config-ipsla-mplslm-react)# react connection-loss
Router(config-ipsla-mplslm-react-cond)# threshold type consecutive 2
```

threshold type immediate

To take action immediately upon a threshold violation, use the **threshold type immediate** command in the appropriate configuration mode. To clear the threshold type (reaction will never happen), use the **no** form of this command.

threshold type immediate
no threshold type

Syntax Description

This command has no keywords or arguments.

Command Default

If there is no default value, no threshold type is configured.

Command Modes

IP SLA reaction condition configuration

IP SLA MPLS LSP monitor reaction condition configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

When the reaction conditions, such as threshold violations, are met for the monitored element, the action is immediately performed as defined by the **action** command.

If the **threshold type immediate** command is used in IP SLA reaction condition mode, it configures the threshold for the specific operation being configured. If the **threshold type immediate** command is used in IP SLA MPLS LSP monitor reaction condition configuration mode, it configures the threshold for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **threshold type immediate** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react  jitter-average
Router(config-ipsla-react-cond)# threshold type immediate
```

The following example shows how to use the **threshold type immediate** command in IP SLA MPLS LSP monitor reaction condition configuration mode:

```
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# reaction monitor 2
Router(config-ipsla-mplslm-react)# react connection-loss
Router(config-ipsla-mplslm-react-cond)# threshold type immediate
```

threshold type xofy

To take action upon X violations in Y probe operations, use the **threshold type xofy** command in IP SLA reaction condition configuration mode. To clear the threshold type (reaction will never happen), use the **no** form of this command.

threshold type xofy *x-value y-value*
no threshold type

Syntax Description

x-value y-value	When the reaction conditions, such as threshold violations, are met for the monitored element after some *x* number of violations within some other *y* number of probe operations (for example, *x* of *y*), the action is performed as defined by the **action** command. Default is 5 for both *x-value* and *y-value;* for example, **xofy** *5 5*. Range is 1 to 16.

Command Default

If there is no default value, no threshold type is configured.

Command Modes

IP SLA reaction condition configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **threshold type xofy** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# reaction operation 432
Router(config-ipsla-react)# react jitter-average
Router(config-ipsla-react-cond)# threshold type xofy 1 5
```

timeout (IP SLA)

To set the probe or control timeout interval, use the **timeout** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

timeout *milliseconds*
no timeout

Syntax Description

milliseconds	Sets the amount of time (in milliseconds) that the IP SLA operation waits for a response from the request packet. Range is 1 to 604800000.

Command Default

None.

Command Modes

IP SLA UDP echo configuration

IP SLA UDP jitter configuration

IP SLA ICMP path-jitter configuration

IP SLA ICMP path-echo configuration

IP SLA ICMP echo configuration

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

IP SLA MPLS LSP monitor ping configuration

IP SLA MPLS LSP monitor trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

If the **timeout** command is used in IP SLA operation mode, it configures the amount of time that a specific IP SLA operation waits for a response from the request packet. If the **timeout** command is used in IP SLA MPLS LSP monitor mode, it configures the amount of time that all operations associated with the monitored provider edge (PE) routers wait for a response from the request packet. This configuration is inherited by all LSP operations that are created automatically.

Note The IP SLA responder needs at least one second to open a socket and program Local Packet Transport Services (LPTS). Therefore, configure the IP SLA timeout to at least 2000 milli seconds.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **timeout** command in IP SLA UDP jitter configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# timeout 10000
```

The following example shows how to use the **timeout** command in IP SLA MPLS LSP monitor configuration mode:

```
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 2
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)# timeout 10000
```

tos

To set the type of service (ToS) in a probe packet, use the **tos** command in the appropriate configuration mode. To use the default value, use the **no** form of this command.

tos *number*
no tos

Syntax Description

number	Type of service number. Range is 0 to 255.

Command Default

The type of service number is 0.

Command Modes

IP SLA UDP echo configuration

IP SLA UDP jitter configuration

IP SLA ICMP path-jitter configuration

IP SLA ICMP path-echo configuration

IP SLA ICMP echo configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The ToS value is an 8-bit field in IP headers. The field contains information, such as precedence and ToS. The information is useful for policy routing and for features like Committed Access Rate (CAR) in which routers examine ToS values. When the type of service is defined for an operation, the IP SLA probe packet contains the configured tos value in the IP header.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **tos** command in IP SLA UDP jitter configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# tos 60
```

ttl

To specify the time-to-live (TTL) value in the MPLS label of echo request packets, use the **ttl** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

ttl *time-to-live*
no ttl

Syntax Description

time-to-live	Maximum hop count for an echo request packet. Valid values are from 1 to 255.

Command Default

For an MPLS LSP ping operation, the default time-to-live value is 255.

For an MPLS LSP trace operations, the default time-to-live value is 30.

Command Modes

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

IP SLA MPLS LSP monitor ping configuration

IP SLA MPLS LSP monitor trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **ttl** command to set the maximum number of hops allowed for echo request packets in an MPLS LSP ping or MPLS LSP trace operation. Note that the number of possible hops differs depending the type of IP SLA operation:

- For MPLS LSP ping operations, valid values are from 1 to 255 and the default is 255.
- For MPLS LSP trace operations, valid values are from 1 to 30 and the default is 30.

If the **ttl** command is used in IP SLA operation mode, it configures the time-to-live value for the specific operation being configured. If the **ttl** command is used in IP SLA MPLS LSP monitor mode, it configures the time-to-live value for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **ttl** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
```

```
Router(config-ipsla-op)# type mpls lsp ping
Router(config-ipsla-mpls-lsp-ping)# ttl 200
```

type icmp echo

To use the ICMP echo operation type, use the **type icmp echo** command in IP SLA operation configuration mode. To remove the operation, use the **no** form of this command.

type icmp echo
no type icmp echo

Syntax Description This command has no keywords or arguments.

Command Default No default behavior or values

Command Modes IP SLA operation configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples The following example shows how to use the **type icmp echo** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type icmp echo
Router(config-ipsla-icmp-echo)#
```

type icmp path-echo

To use the ICMP path-echo operation type, use the **type icmp path-echo** command in IP SLA operation configuration mode. To remove the operation, use the **no** form of this command.

type icmp path-echo
no type icmp path-echo

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes IP SLA operation configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples The following example shows how to use the **type icmp path-echo** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type icmp path-echo
Router(config-ipsla-icmp-path-echo)#
```

type icmp path-jitter

To use the ICMP path-jitter operation type, use the **type icmp path-jitter** command in IP SLA operation configuration mode. To remove the operation, use the **no** form of this command.

type icmp path-jitter
no type icmp path-jitter

Syntax Description This command has no keywords or arguments.

Command Default No default behavior or values

Command Modes IP SLA operation configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **type icmp path-jitter** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type icmp path-jitter
Router(config-ipsla-icmp-path-jitter)#
```

type mpls lsp ping

To verify the end-to-end connectivity of a label switched path (LSP) and the integrity of an MPLS network, use the **type mpls lsp ping** command in the appropriate configuration mode. To remove the operation, use the **no** form of this command.

type mpls lsp ping
no type mpls lsp ping

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

IP SLA operation configuration

IP SLA MPLS LSP monitor definition configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **type mpls lsp ping** command to configure parameters for an IP SLA LSP ping operation. After you enter the command, you enter IP SLA MPLS LSP Ping configuration mode.

An MPLS LSP ping operation tests connectivity between routers along an LSP path in an MPLS network and measures round-trip delay of the LSP by using an echo request and echo reply.

The MPLS LSP ping operation verifies LSP connectivity by using one of the supported Forwarding Equivalence Class (FEC) entities between the ping origin and egress node of each FEC. The following FEC types are supported for an MPLS LSP ping operation:

- IPv4 LDP prefixes (configured with the target ipv4, on page 88 command)
- MPLS TE tunnels (configured with the target traffic-eng , on page 91 command)
- Pseudowire (configured with the target pseudowire, on page 90 command)

For MPLS LSP monitor ping operations, only IPv4 LDP prefixes are supported.

If the **type mpls lsp ping** command is used in IP SLA operation configuration mode, it configures the parameters for the specific operation being configured. If the **type mpls lsp ping** command is used in IP SLA MPLS LSP monitor configuration mode, it configures the parameters for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **type mpls lsp ping** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp ping
Router(config-ipsla-mpls-lsp-ping)#
```

The following example shows how to use the **type mpls lsp ping** command in IP SLA MPLS LSP monitor configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 2
Router(config-ipsla-mplslm-def)# type mpls lsp ping
Router(config-ipsla-mplslm-lsp-ping)#
```

type mpls lsp trace

To trace LSP paths and localize network faults in an MPLS network, use the **type mpls lsp trace** command in the appropriate configuration mode. To remove the operation, use the **no** form of this command.

type mpls lsp trace
no type mpls lsp trace

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

IP SLA operation configuration

IP SLA MPLS LSP monitor definition configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **type mpls lsp trace** command to configure parameters for an IP SLA LSP trace operation. After you enter the command, you enter IP SLA MPLS LSP Trace configuration mode.

An MPLS LSP trace operation traces the hop-by-hop route of LSP paths to a target router and measures the hop-by-hop round-trip delay for IPv4 LDP prefixes and TE tunnel FECs in an MPLS network. Echo request packets are sent to the control plane of each transit label switching router (LSR). A transit LSR performs various checks to determine if it is a transit LSR for the LSP path. A trace operation allows you to troubleshoot network connectivity and localize faults hop-by-hop.

In an MPLS LSP trace operation, each transit LSR returns information related to the type of Forwarding Equivalence Class (FEC) entity that is being traced. This information allows the trace operation to check if the local forwarding information matches what the routing protocols determine as the LSP path.

An MPLS label is bound to a packet according to the type of FEC used for the LSP. The following FEC types are supported for an MPLS LSP trace operation:

- LDP IPv4 prefixes (configured with the target ipv4, on page 88 command)
- MPLS TE tunnels (configured with the target traffic-eng , on page 91 command)

For MPLS LSP monitor trace operations, only IPv4 LDP prefixes are supported.

If the **type mpls lsp trace** command is used in IP SLA operation configuration mode, it configures the parameters for the specific operation being configured. If the **type mpls lsp trace** command is used in IP SLA MPLS LSP monitor configuration mode, it configures the parameters for all operations associated with the monitored provider edge (PE) routers. This configuration is inherited by all LSP operations that are created automatically.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **type mpls lsp trace** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type mpls lsp trace
Router(config-ipsla-mpls-lsp-trace)#
```

The following example shows how to use the **type mpls lsp trace** command in IP SLA MPLS LSP monitor configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 2
```

```
Router(config-ipsla-mplslm-def)# type mpls lsp trace
Router(config-ipsla-mplslm-lsp-trace)#
```

type udp echo

To use the UDP echo operation type, use the **type udp echo** command in IP SLA operation configuration mode. To remove the operation, use the **no** form of this command.

type udp echo
no type udp echo

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes IP SLA operation configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples The following example shows how to use the **type udp echo** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp echo
Router(config-ipsla-udp-echo)#
```

type udp jitter

To use the UDP jitter operation type, use the **type udp jitter** command in IP SLA operation configuration mode. To remove the operation, use the **no** form of this command.

type udp jitter
no type udp jitter

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes IP SLA operation configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples The following example shows how to use the **type udp jitter** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)#
```

type udp ipv4 address

To configure a permanent port in the IP SLA responder for UDP echo or jitter operations, use the **type udp ipv4 address** command in IP SLA responder configuration mode. To remove the specified permanent port, use the **no** form of this command.

type udp ipv4 address *ip-address* **port** *port*
no type udp ipv4 address *ip-address* **port** *port*

Syntax Description

ip-address	Specifies the IPv4 address at which the operation is received.
port *port*	Specifies the port number at which the operation is received. Range is identical to the one used for the subagent that is, 1 to 65355.

Command Default If there is no default value, no permanent port is configured.

Command Modes IP SLA responder configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to configure a permanent port for the **type udp ipv4 address** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# responder
Router(config-ipsla-resp)# type udp ipv4 address 192.0.2.11 port 10001
```

verify-data

To check each IP SLA response for corruption, use the **verify-data** command in the appropriate configuration mode. To disable data corruption checking, use the **no** form of this command.

verify-data
no verify-data

Syntax Description

This command has no keywords or arguments.

Command Default

The **verify-data** command is disabled.

Command Modes

IP SLA UDP echo configuration

IP SLA UDP jitter configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **verify-data** command in IP SLA UDP jitter configuration mode:

```
Router# configure
Router(config)# ipsla
```

```
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# verify-data
```

vrf (IP SLA)

To enable the monitoring of a Virtual Private Network (VPN) in an ICMP echo, ICMP path-echo, ICMP path-jitter, UDP echo, or UDP jitter operation, use the **vrf** command in the appropriate configuration mode. To disable VPN monitoring, use the **no** form of this command.

vrf *vrf-name*
no vrf

Syntax Description

vrf-name	Name of the VPN. Maximum length is 32 alphanumeric characters.

Command Default

VPN monitoring is not configured for an IP SLA operation.

Command Modes

IP SLA ICMP path-jitter configuration

IP SLA ICMP path-echo configuration

IP SLA ICMP echo configuration

IP SLA UDP echo configuration

IP SLA UDP jitter configuration

IP SLA MPLS LSP ping configuration

IP SLA MPLS LSP trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

Use the **vrf** command to configure a non-default VPN routing and forwarding (VRF) table for an IP SLA operation. A VPN is commonly identified using the name of a VRF table. If you use the **vrf** command in the configuration of an IP SLA operation, the *vrf-name* value is used to identify the VPN for the particular operation.

The default VRF table is used if no value is specified with the **vrf** command. If you enter a VPN name for an unconfigured VRF, the IP SLA operation fails and the following information is displayed in the results for the show ipsla statistics, on page 69 command:

```
Latest operation return code  : VrfNameError
```

The **vrf** command is supported only to configure the following IP SLA operations:

- IP SLA ICMP echo
- IP SLA ICMP path-echo

- IP SLA ICMP path-jitter
- IP SLA UDP echo
- IP SLA UDP jitter
- IP SLA MPLS LSP ping
- IP SLA MPLS LSP trace

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **vrf** command:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# operation 1
Router(config-ipsla-op)# type udp jitter
Router(config-ipsla-udp-jitter)# vrf vpn2
```

vrf (IP SLA MPLS LSP monitor)

To specify which virtual routing and forwarding instance (VRF) is monitored in an IP SLA MPLS LSP monitor ping or trace, use the **vrf** command in the the appropriate configuration mode. To revert to the monitoring of all VRFs, use the **no** form of this command.

vrf *vrf-name*
no vrf

Syntax Description

vrf-name	Name of the VRF. Maximum length is 32 alphanumeric characters.

Command Default

All VRFs are monitored.

Command Modes

IP SLA MPLS LSP monitor ping configuration

IP SLA MPLS LSP monitor trace configuration

Command History

Release	Modification
Release 7.3.2	This command was introduced.

Usage Guidelines

The **vrf** command in IP SLA MPLS LSP monitor configuration mode specifies to monitor a specific VRF in ping and trace operations. The default is that all VRFs are monitored.

Task ID

Task ID	Operations
monitor	read, write

Examples

The following example shows how to use the **vrf** command in IP SLA MPLS LSP monitor configuration mode:

```
Router# configure
Router(config)# ipsla
Router(config-ipsla)# mpls lsp-monitor
Router(config-ipsla-mplslm)# monitor 2
Router(config-ipsla-mplslm-def)# type mpls lsp trace
Router(config-ipsla-mplslm-lsp-trace)# vrf vpn-lsp
```