mpls traffic-eng lsp attributes through route-target

mpls traffic-eng lsp attributes

To create or modify a label switched path (LSP) attribute list, use the**mpls traffic-eng lsp attributes** command in global configuration mode. To remove a specified LSP attribute list from the device configuration, use the **no** form of this command.

mpls traffic-eng lsp attributes *string*
no mpls traffic-eng lsp attributes *string*

Syntax Description

string	LSP attributes list identifier.

Command Default

An LSP attribute list is not created unless you create one.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command sets up an LSP attribute list and enters LSP Attributes configuration mode, in which you can enter LSP attributes.

To associate the LSP attributes and LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option attributes** *string* command, where *string* is the identifier for the specific LSP attribute list.

An LSP attribute referenced by the path option takes precedence over the values configured on the tunnel interface. If an attribute is not specified in the LSP attribute list, the devices takes the attribute from the tunnel configuration. LSP attribute lists do not have default values. If the attribute is not configured on the tunnel, then the device uses tunnel default values.

Once you type the **mpls traffic-eng lsp attributes** command, you enter the LSP Attributes configuration mode where you define the attributes for the LSP attribute list that you are creating.

The mode commands are as follows:

- **affinity**—Specifies attribute flags for links that make up an LSP.
- **auto-bw**—Specifies automatic bandwidth configuration.
- **bandwidth**—Specifies LSP bandwidth.
- **lockdown**—Disables reoptimization for the LSP.
- **priority**—Specifies LSP priority.

- **protection**—Enables failure protection.
- **record-route**—Records the route used by the LSP.

The following monitoring and management commands are also available in the LSP Attributes configuration mode:

- **exit**—Exits from LSP Attributes configuration mode.
- **list**—Relists all the entries in the LSP attribute list.
- **no**—Removes a specific attribute from the LSP attribute list.

Examples

The following example shows how to set up an LSP attribute list identified with the numeral 6 with the **bandwidth** and **priority** mode commands. The example also shows how to use the **list** mode command:

```
Device(config)# mpls traffic-eng lsp attributes 6
Device(config-lsp-attr)# bandwidth 500
Device(config-lsp-attr)# list
LIST 6
 bandwidth 500

Device(config-lsp-attr)# priority 1 1
Device(config-lsp-attr)# list
LIST 6
 bandwidth 500
 priority 1 1
Device(config-lsp-attr)# exit
```

Related Commands

Command	Description
show mpls traffic-eng lsp attributes	Displays global LSP attributes lists.

mpls traffic-eng mesh-group

To configure a mesh group in an Interior Gateway Protocol (IGP) to allow Multiprotocol Label Switching (MPLS) traffic engineering (TE) label switch routers (LSRs) that belong to the same mesh group to signal tunnels to the local router, use the **mpls traffic-eng mesh-group** command in router configuration mode. To disable signaling of tunnels from LSRs in the same mesh group to the local router, use the **no** form of this command.

mpls traffic-eng mesh-group *mesh-group-id type number* **area** *area-id*
no mpls traffic-eng mesh-group *mesh-group-id type number* **area** *area-id*

Syntax Description

mesh-group-id	Number that identifies a specific mesh group.
type	Type of interface.
number	Interface number.
area *area-id*	Specifies an IGP area.

Command Default

No tunnels are signaled for routers in the same mesh group.

Command Modes

Router configuration (config-router)#

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.

Usage Guidelines

Use this command to configure a mesh group in an IGP. This allows the MPLS TE LSRs that belong to the specified mesh group to signal tunnels to the local router. The IGP floods mesh group configuration to all routers belonging to the same mesh group. An autotemplate determines how a router participates in an autotunnel. A router can participate in a mesh group through two-way tunnels or one-way tunnels.

Open Shortest Path First (OSPF) is the only IGP supported for the MPLS Traffic Engineering--AutoTunnel Mesh Groups feature.

Examples

The following example shows how to configure OSPF to allow LSRs that belong to the same mesh group (mesh group 10) to signal tunnels to the local router:

```
Router(config)# router ospf 100
Router(config-router)# mpls traffic-eng mesh-group 10 loopback 0 area 100
```

Related Commands

Command	Description
tunnel destination mesh-group	Configures an autotemplate to signal tunnels to all other members of a specified mesh group.

mpls traffic-eng multicast-intact

To configure a router running Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF) so that Protocol-Independent Multicast (PIM) and Multiprotocol Label Switching (MPLS) traffic engineering (TE) can work together, use the **mpls traffic-eng multicast-intact** command in router configuration mode. To disable interoperability between PIM and MPLS TE, use the **no** form of this command.

mpls traffic-eng multicast-intact
no mpls traffic-eng multicast-intact

Syntax Description

This command has no arguments or keywords.

Command Default

PIM and MPLS TE do not work together.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(12)S	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **mpls traffic-eng multicast-intact** command allows PIM to use the native hop-by-hop neighbors while unicast routing is using MPLS TE tunnels.

This command works only for OSPF and IS-IS protocols.

Examples

The following example shows how to enable PIM and MPLS TE to interoperate:

```
Router(config)# router ospf 1
Router(config-router)# mpls traffic-eng multicast-intact
```

Related Commands

Command	Description
mpls traffic-eng interface	Configures a router running OSPF or IS-IS so that it floods MPLS TE link information in the indicated OSPF area or IS-IS level.
show ospf routes multicast intact	Displays multicast-intact paths of OSPF routes.

mpls traffic-eng nsr

To enable Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Nonstop Routing (NSR) support on a device, use the **mpls traffic-eng nsr** command in global configuration mode. To disable MPLS TE NSR support, use the **no** form of this command.

mpls traffic-eng nsr

no mpls traffic-eng nsr

This command has no arguments or keywords.

Command Default

MPLS TE NSR support is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS Release XE 3.10S	This command was introduced.

The following example shows how to enable MPLS TE NSR support using the use the **mpls traffic-eng nsr** command.

```
enable
 configure terminal
  ip cef
  mpls traffic-eng nsr
  end
```

Related Commands

Command	Description
show mpls traffic-eng nsr	Displays information about MPLS TE NSR.

mpls traffic-eng passive-interface

To configure a link as a passive interface between two Autonomous System Boundary Routers (ASBRs), use the **mpls traffic-eng passive-interface** command in interface configuration mode. To disable the passive link, use the **no** form of this command.

mpls traffic-eng passive-interface nbr-te-id *te-router-id* [**nbr-if-addr** *if-addr*] [**nbr-igp-id** {**isis** *sysid* | **ospf** *sysid*}]
no mpls traffic-eng passive-interface nbr-te-id *te-router-id* [**nbr-if-addr** *if-addr*] [**nbr-igp-id** {**isis** *sysid* | **ospf** *sysid*}]

Syntax Description

nbr-te-id *te-router-id*	Traffic engineering router ID of the neighbor router on the remote side of the link where this command is configured.
nbr-if-addr *if-addr*	(Optional) Interface address of the remote ASBR.
nbr-igp-id	(Optional) Specifies a unique *sysid* for neighboring Interior Gateway Protocols (IGPs) when two or more autonomous systems use different IGPs and have more than one neighbor on the link. Enter the **nbr-igp-id** keyword (followed by the **isis** or **ospf** keyword) and the *sysid* for each IGP. The *sysid* must be unique for each neighbor.
isis *sysid*	System identification of Intermediate System-to-Intermediate System (IS-IS).
ospf *sysid*	System identification of Open Shortest Path First (OSPF).

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	The **nbr-if-addr** keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

The **mpls traffic-eng passive-interface** command sets the next-hop address for a passive interface. The command is required only for a broadcast link.

Enter the **mpls traffic-eng passive-interface** command only on the outgoing interface on which the label-switched path (LSP) will exit; you do not have to enter this command on both ends of the interautonomous system (Inter-AS) link.

On a point-to-point link or on a multiaccess link where there is only one neighbor, you do not have to enter the **isis** or **ospf** keyword (or the *sysid* argument).

If two autonomous systems use different IGPs and have more than one neighbor on the link, you must enter the **nbr-igp-id** keyword followed by **isis** or **ospf** and the *sysid*. The *sysid* must be unique for each neighbor.

For a broadcast link (that is, other Resource Reservation Protocol (RSVP)) features are using the passive link), you must enter the **nbr-if-addr** keyword.

For an RSVP Hello configuration on an Inter-AS link, all keywords are required.

Examples

In the following example there is only one neighbor:

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.10.10
```

In the following example, two autonomous systems use different IGPs and have more than one neighbor on the link:

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.11.12 nbr-igp-id ospf
 10.10.15.18
```

If autonomous system 1 (AS1) is running IS-IS and AS2 is running OSPF, the unique ID on A1 must be in the system ID format. To form the system ID, we recommend that you append zeros to the router ID of the neighbor. For example, if the AS2 router is 10.20.20.20, then you could enter a system ID of 10.0020.0020.0020.00 for IS-IS on the AS1 router.

In the following example there is a remote ASBR and an IS-IS:

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.20.20.20 nbr-igp-id isis
 10.0020.0020.0020.00
```

In the following example, there is a broadcast link and the interface address of the remote ASBR is 10.0.0.2:

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.10.10 nbr-if-addr
10.0.0.2
```

mpls traffic-eng path-option list

To configure a path option list, use the **mpls traffic-eng path-option list** command in global configuration mode. To disable this function, use the **no** form of this command.

mpls traffic-eng path-option list [{**name** *pathlist-name* | **identifier** *pathlist-number*}]
no mpls traffic-eng path-option list [{**name** *pathlist-name* | **identifier** *pathlist-number*}]

Syntax Description

name *pathlist-name*	Specifies the name of the path option list.
identifier *pathlist-number*	Specifies the identification number of the path option list. The range is 1 through 65535.

Command Default

There are no path option lists.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

A path option list contains a list of backup paths for a primary path option. You can specify a path option list by entering its name or identifier.

After you enter the **mpls traffic-eng path-option list** command, the router enters path option list configuration mode and you can enter the following commands:

- **path-option** --Specifies the name or identification number of the next path option to add, edit, or delete.
- **list** --Lists all path options.
- **no** --Deletes a specified path option.
- **exit** --Exits from path option list configuration mode.

Then you can specify explicit backup paths by entering their name or identifier.

Examples

The following example configures the path option list named pathlist-01, adds path option 10, lists the backup path that is in the path option list, and exits from path option list configuration mode:

```
Router(config)# mpls traffic-eng path-option list name pathlist-01
Router(cfg-pathoption-list)# path-option 10 explicit name bk-path-01
Router(cfg-pathoption-list)# list
 path-option 10 explicit name bk-path-01
Router(cfg-pathoption-list)# exit
```

Related Commands

Command	Description
tunnel mpls traffic-eng path option	Configures a path option for an MPLS TE tunnel.
tunnel mpls traffic-eng path-option protect	Configures a secondary path option or a path option list for an MPLS TE tunnel.

mpls traffic-eng path-selection metric

To specify the metric type to use for path selection for tunnels for which the metric type has not been explicitly configured, use the **mpls traffic-eng path-selection metric** command in global configuration mode. To remove the specified metric type, use the **no** form of this command.

mpls traffic-eng path-selection metric {**igp** | **te**}
no mpls traffic-eng path-selection metric

Syntax Description

igp	Use the Interior Gateway Protocol (IGP) metric.
te	Use the traffic engineering metric.

Command Default

The default is the **te** metric.

Command Modes

Global configuration

Command History

Release	Modification
12.0(18)ST	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to specify the metric type to be used for traffic engineering (TE) tunnels for which the **tunnel mpls traffic-eng path-selection metric** command has not been specified.

The metric type to be used for path calculation for a given tunnel is determined as follows:

- If the **tunnel mpls traffic-eng path-selection metric** command was entered to specify a metric type for the tunnel, use that metric type.
- Otherwise, if the **mpls traffic-eng path-selection metric** was entered to specify a metric type, use that metric type.
- Otherwise, use the default (**te**) metric.

Examples

The following command specifies that if a metric type was not specified for a given TE tunnel, the igp metric should be used for tunnel path calculation:

```
Router(config)# mpls traffic-eng path-selection metric igp
```

Related Commands

Command	Description
tunnel mpls traffic-eng path-selection metric	Specifies the metric type to use when calculating a tunnel's path.

mpls traffic-eng reoptimize

To force immediate reoptimization of all traffic engineering tunnels, use the **mpls traffic-eng reoptimize** command in privileged EXEC mode.

mpls traffic-eng reoptimize

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)ST	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to reoptimize all traffic engineering tunnels immediately:

```
Router# mpls traffic-eng reoptimize
```

Related Commands

Command	Description
mpls traffic-eng reoptimize timers delay	Delays removal of old LSPs or installation of new LSPs after tunnel reoptimization.

mpls traffic-eng reoptimize events

To turn on automatic reoptimization of Multiprotocol Label Switching (MPLS) traffic engineering when certain events occur, such as when an interface becomes operational, use the **mpls traffic-eng reoptimize events** command in global configuration mode. To disable automatic reoptimization, use the **no** form of this command.

mpls traffic-eng reoptimize events link-up
no mpls traffic-eng reoptimize events link-up

Syntax Description

link-up	Triggers automatic reoptimization whenever an interface becomes operational.

Command Default

Event-based reoptimization is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to turn on automatic reoptimization whenever an interface becomes operational:

```
Router(config)# mpls traffic-eng reoptimize events link-up
```

Related Commands

Command	Description
mpls traffic-eng logging lsp	Controls the frequency with which tunnels with established LSPs are checked for better LSPs.
mpls traffic-eng reoptimize	Reoptimizes all traffic engineering tunnels immediately.
mpls traffic-eng reoptimize timers delay	Delays removal of old LSPs or installation of new LSPs after tunnel reoptimization.

mpls traffic-eng reoptimize timers delay

To delay the removal of old label switched paths (LSPs) or installation of new LSPs after tunnel reoptimization, use the **mpls traffic-eng reoptimize timers delay** command in global configuration mode. To restore the default value, use the **no** form of this command.

mpls traffic-eng reoptimize timers delay {**cleanup** *delay-time* | **installation** *delay-time*}
no mpls traffic-eng reoptimize timers delay {**cleanup** *delay-time* | **installation** *delay-time*}

Syntax Description

cleanup *delay-time*	Delays the removal of old LSPs after tunnel reoptimization for the specified number of seconds. The range is from 0 to 300. A value of 0 disables the delay. The default is 10.
installation *delay-time*	Delays the installation of new LSPs with new labels, for the specified number of seconds, after tunnel reoptimization. The range is from 0 to 3600. A value of 0 disables the delay. The default is 3.

Command Default

Removal of old LSPs and installation of new LSPs is not delayed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(32)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE7	This command was integrated into Cisco IOS Release 12.2(33)SRE7. The maximum value for the **cleanup** *delay-time* argument was changed from 60 to 300 seconds.
15.0(1)S6	This command was modified. The maximum value for the **cleanup** *delay-time* argument was changed from 60 to 300 seconds.

Usage Guidelines

A device with Multiprotocol Label Switching traffic engineering (MPLS-TE) tunnels periodically examines tunnels with established LSPs to discover if more efficient LSPs (paths) are available. If a better LSP is available, the device signals the more efficient LSP. If the signaling is successful, the device replaces the older LSP with the new, more efficient LSP.

Sometimes, the slower router-point nodes may not utilize the new label's forwarding plane. In this case, if the headend node replaces the labels quickly, packet loss can occur. The packet loss is avoided by delaying the cleanup of the old LSP by using the **mpls traffic-eng reoptimize timers delay cleanup** command. Until the cleanup of the old LSP is performed, subsequent reoptimizations for the tunnel are prevented.

Examples

The following example shows how to set the reoptimization cleanup delay time to one minute:

```
Device# configure terminal
Device(config)# mpls traffic-eng reoptimize timers delay cleanup 60
```

The following example shows how to set the reoptimization installation delay time to one hour:

```
Device# configure terminal
Device(config)# mpls traffic-eng reoptimize timers delay installation 3600
```

Related Commands

Command	Description
mpls traffic-eng reoptimize	Forces immediate reoptimization of all traffic engineering tunnels.
mpls traffic-eng reoptimize events	Turns on automatic reoptimization of MPLS traffic engineering when certain events occur, such as when an interface becomes operational.
mpls traffic-eng reoptimize timers frequency	Controls the frequency with which tunnels with established LSPs are checked for better LSPs.

mpls traffic-eng reoptimize timers frequency

To control the frequency with which tunnels with established label switched paths (LSPs) are checked for better LSPs, use the **mpls traffic-eng reoptimize timers frequency** command in global configuration mode. To disable this function, use the **no** form of this command.

mpls traffic-eng reoptimize timers frequency *seconds*
no mpls traffic-eng reoptimize timers frequency

Syntax Description

seconds	Sets the frequency of reoptimization (in seconds). A value of 0 disables reoptimization. The range is 0 to 604800 seconds (1 week).

Command Default

3600 seconds (1 hour)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A device with traffic engineering tunnels periodically examines tunnels with established LSPs to learn if better LSPs are available. If a better LSP seems to be available, the device attempts to signal the better LSP; if the signaling is successful, the device replaces the old, inferior LSP with the new, better LSP.

Note If the **lockdown** keyword is specified with the **tunnel mpls traffic-eng path-option** command, then a reoptimize check is not done on the tunnel.

If you configure a traffic engineering tunnel with an explicit path that is not fully specified (a series of router IDs or a combination of router IDs and interface addresses), then reoptimization may not occur.

Note If you specify a low reoptimization frequency (for example, less than 30 seconds), there may be an increase in CPU utilization for configurations with a large number of traffic engineering tunnels.

Examples

The following example shows how to set the reoptimization frequency to 1 day:

```
Router(config)# mpls traffic-eng reoptimize timers frequency 86400
```

Related Commands

Command	Description
mpls traffic-eng reoptimize	Reoptimizes all traffic engineering tunnels immediately.
mpls traffic-eng reoptimize timers delay	Delays removal of old LSPs or installation of new LSPs after tunnel reoptimization.
tunnel mpls traffic-eng path-option	Configures a path option for an MPLS traffic engineering tunnel.

mpls traffic-eng router-id

To specify that the traffic engineering router identifier for the node is the IP address associated with a given interface, use the **mpls traffic-eng router-id** command in router configuration mode. To remove the traffic engineering router identifier, use the **no** form of this command.

mpls traffic-eng router-id *interface-name*
no mpls traffic-eng router-id

Syntax Description

interface-name	Interface whose primary IP address is the router's identifier.

Command Default

No traffic engineering router identifier is specified.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This router identifier acts as a stable IP address for the traffic engineering configuration. This IP address is flooded to all nodes. For all traffic engineering tunnels originating at other nodes and ending at this node, you must set the tunnel destination to the traffic engineering router identifier of the destination node, because that is the address that the traffic engineering topology database at the tunnel head uses for its path calculation.

You should configure the same traffic engineering router id for all Interior Gateway Protocol (IGP) routing processes.

Examples

The following example shows how to specify the traffic engineering router identifier as the IP address associated with interface Loopback0:

```
Router(config-router)# mpls traffic-eng router-id Loopback0
```

Related Commands

Command	Description
mpls atm control-vc	Turns on flooding of MPLS traffic engineering link information in the indicated IGP level/area.

mpls traffic-eng scanner

To specify how often Intermediate System-to-Intermediate System (IS-IS) extracts traffic engineering type, length, values (TLVs) objects from flagged label switched paths (LSPs) and passes them to the traffic engineering topology database, and the maximum number of LSPs that the router can process immediately, use the **mpls traffic-eng scanner** command in router configuration mode. To disable the frequency that IS-IS extracts traffic engineering TLVs and the maximum number of LSPs IS-IS passes to the traffic engineering topology database, use the **no** form of this command.

mpls traffic-eng scanner [**interval seconds**] [**max-flash LSPs**]
no mpls traffic-eng scanner

Syntax Description

interval *seconds*	(Optional) Frequency, in seconds, at which IS-IS sends traffic engineering TLVs into the traffic engineering database. The range is 1 to 60. The default value is 5.
max-flash *LSPs*	(Optional) Maximum number of LSPs that the router can process immediately without incurring a delay. The range is 0 to 200. The default value is 15.

Command Default

IS-IS sends traffic engineering TLVs into the traffic engineering topology database every 5 seconds after the first 15 LSPs are processed.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

When IS-IS receives a new LSP, it inserts it into the IS-IS database. If the LSP contains traffic engineering TLVs, IS-IS flags the LSPs for transmission to the traffic engineering database. Depending on the default or user-specified interval, traffic engineering TLVs are extracted and sent to the traffic engineering database. Users can also specify the maximum number of LSPs that the router can process immediately. Processing

entails checking for traffic engineering TLVs, extracting them, and passing them to the traffic engineering database. If more than 50 LSPs need to be processed, there is a delay of 5 seconds for subsequent LSPs.

The first 15 LSPs are sent without a delay into the traffic engineering database. If more LSPs are received, the default delay of 5 seconds applies.

If you specify the **no** form of this command, there is a delay of 5 seconds before IS-IS scans its database and passes traffic engineering TLVs associated with flagged LSPs to the traffic engineering database

Examples

In the following example, the router is allowed to process up to 50 IS-IS LSPs without any delay.

```
Router(config)# router isis
Router(config-router)# mpls traffic-eng scanner interval 5 max-flash 50
```

Related Commands

Command	Description
mpls traffic-eng	Configures a router running IS-IS so that it floods MPLS traffic engineering link information into the indicated IS-IS level.
mpls traffic-eng router-id	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

mpls traffic-eng signalling advertise explicit-null

Note Effective with Cisco IOS Release 15.2(2)S, the **mpls traffic-eng signalling advertise implicit-null** command is deprecated by the **mpls traffic-eng signalling advertise explicit-null** command because the IOS MPLS-TE tail router now advertises the implicit-null label in signaling messages sent to neighbors by default. Prior to this release, the IOS MPLS-TE tail router advertised the explicit-null label by default.

To configure the MPLS-TE tail router to override the new default (implicit-null label) to use the MPLS encoding for the explicit-null label in signaling messages advertised to neighbors, use the **mpls traffic-eng signalling advertise explicit-null** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng signalling advertise explicit-null [{*acl-number*}]
no mpls traffic-eng signalling advertise explicit-null

Syntax Description

acl-number	(Optional) Matches the number of the IP access list to determine applicable signalling peers.

Command Default

The IOS MPLS-TE tail router now advertises the implicit-null label in signaling messages sent to neighbors.

Command Modes

Global configuration (config)#

Command History

Release	Modification
15.2(2)S	This command was introduced. This command replaces the **mpls traffic-eng signalling advertise implicit-null** command.
Cisco IOS-XE Release 3.6	This command was introduced.

Usage Guidelines

If the **mpls traffic-eng signalling advertise implicit-null** command exists your configuration we recommend that you remove it from your configuration.

The **mpls traffic-eng signalling advertise explicit-null** command is used on an IOS or IOS-XE MPLS-TE tail router to advertise explicit-null label in signaling messages. If the **mpls traffic-eng signalling advertise explicit-null** command is not configured, an implicit-null label (IETF label 3) is advertised in signaling messages.

Examples

The following example shows how to configure the router to use MPLS encoding for the explicit-null label when it sends signaling messages to all peers:

```
Router(config)# mpls traffic-eng signalling advertise explicit-null
```

mpls traffic-eng signalling advertise implicit-null

Note Effective with Cisco IOS Release 15.2(2)S, the **mpls traffic-eng signalling advertise implicit-null** command is deprecated by the **mpls traffic-eng signalling advertise explicit-null** command because the IOS MPLS-TE tail router now advertises the implicit-null label in signaling messages sent to neighbors by default. Prior to this release, the IOS MPLS-TE tail router advertised the explicit-null label by default. See the **mpls traffic-eng signalling advertise explicit-null** command if you want to configure the IOS MPLS-TE tail router to override the new default (implicit-null label) and advertise the explicit-null label to neighbors instead.

To use MPLS encoding for the implicit-null label in signaling messages sent to neighbors, use the **mpls traffic-eng signalling advertise implicit-null** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng signalling advertise implicit-null [{*acl-number*}]
no mpls traffic-eng signalling advertise implicit-null

Syntax Description

acl-number	(Optional) Matches the number of the IP access list to determine applicable signalling peers.

Command Default

None

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.0(5)ST	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.2(2)S	This command was replaced by the **mpls traffic-eng signalling advertise explicit-null** command.

Usage Guidelines

The **mpls traffic-eng signalling advertise implicit-null** command is typically used on an IOS MPLS-TE tail router to advertise the IETF implicit-null label "3" signalling message to an non-IOS router.

Examples

The following example shows how to configure the router to use MPLS encoding for the implicit-null label when it sends signaling messages to certain peers:

```
Router(config)# mpls traffic-eng signalling advertise implicit-null
```

mpls traffic-eng srlg

To configure the Shared Risk Link Group (SRLG) membership of a link (interface), use the **mpls traffic-eng srlg** command in interface configuration mode. To remove a link from membership of one or more SRLGs, use the **no** form of this command.

mpls traffic-eng srlg [*num*]
no mpls traffic-eng srlg [*num*]

Syntax Description

num	(Optional) SRLG identifier. The range is 0 to 4294967295.

Command Default

A link does not have membership in any SRLG.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S.

Usage Guidelines

You can enter the **mpls traffic-eng srlg** command multiple times to make a link a member of multiple SRLGs.

Examples

The following example makes the interface a member of SRLG 5:

```
Router(config-if)# mpls traffic-eng srlg 5
```

If you enter the following commands, the interface is a member of both SRLG 5 and SRLG 6:

```
Router(config-if)# mpls traffic-eng srlg 5
Router(config-if)# mpls traffic-eng srlg 6
```

To remove a link from membership of SRLG 5, enter the following command:

```
Router(config-if)# no mpls traffic-eng srlg 5
```

To remove a link from membership of all SRLGs, enter the following command:

```
Router(config-if)# no mpls traffic-eng srlg
```

Related Commands

Command	Description
mpls traffic-eng auto-tunnel backup srlg exclude	Specifies that autocreated backup tunnels should avoid SRLGs of the protected interface.

mpls traffic-eng topology holddown sigerr

To specify the amount of time that a router ignores a link in its traffic engineering topology database in tunnel path Constrained Shortest Path First (CSPF) computations following a traffic engineering tunnel error on the link, use the **mpls traffic-eng topology holddown sigerr** command in global configuration mode. To disable the time set to ignore a ink following a traffic engineering tunnel error on the link, use the **no** form of this command.

mpls traffic-eng topology holddown sigerr *seconds*
no mpls traffic-eng topology holddown sigerr

Syntax Description

seconds	Length of time (in seconds) a router should ignore a link during tunnel path calculations following a traffic engineering tunnel error on the link. The range is 0 to 300.

Command Default

If you do not specify this command, tunnel path calculations ignore a link on which there is a traffic engineering error until either 10 seconds have elapsed or a topology update is received from the Interior Gateway Protocol (IGP).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

A router that is at the headend for traffic engineering tunnels might receive a Resource Reservation Protocol (RSVP) No Route error message for an existing tunnel or for one being signaled due to the failure of a link the tunnel traffic traverses before the router receives a topology update from the IGP routing protocol announcing that the link is down. In such a case, the headend router ignores the link in subsequent tunnel path calculations to avoid generating paths that include the link and are likely to fail when signaled. The link is ignored until the router receives a topology update from its IGP or a link hold-down timeout occurs. You can use the **mpls traffic-eng topology holddown sigerr** command to change the link hold-down time from its 10-second default value.

Examples

In the following example, the link hold-down time for signaling errors is set at 15 seconds:

```
Router(config)# mpls traffic-eng topology holddown sigerr 15
```

Related Commands

Command	Description
show mpls traffic-eng topology	Displays the MPLS traffic engineering global topology as currently known at the node.

mpls traffic-eng tunnels (global configuration)

To enable Multiprotocol Label Switching (MPLS) traffic engineering tunnel signaling on a device, use the **mpls traffic-eng tunnels** command in global configuration mode. To disable MPLS traffic engineering tunnel signaling, use the **no** form of this command.

mpls traffic-eng tunnels
no mpls traffic-eng tunnels

Syntax Description

This command has no arguments or keywords.

Command Default

The command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

This command enables MPLS traffic engineering on a device. For you to use the feature, MPLS traffic engineering must also be enabled on the desired interfaces.

Examples

The following example shows how to turn on MPLS traffic engineering tunnel signaling:

```
Router(config)# mpls traffic-eng tunnels
```

Related Commands

Command	Description
mpls traffic-eng tunnels (interface configuration)	Enables MPLS traffic engineering tunnel signaling on an interface.

mpls traffic-eng tunnels (interface configuration)

To enable Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel signaling on an interface (assuming that it is enabled on the device), use the **mpls traffic-eng tunnels** command in interface configuration mode. To disable MPLS traffic engineering tunnel signaling on the interface, use the **no** form of this command.

mpls traffic-eng tunnels

no mpls traffic-eng tunnels

Syntax Description

This command has no arguments or keywords.

Command Default

The MPLS TE is disabled on all interfaces.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Before you enable MPLS TE on the interface, you must enable MPLS TE on the device. An enabled interface has its resource information flooded into the appropriate Interior Gateway Protocol (IGP) link-state database and accepts traffic engineering tunnel signaling requests.

You can use this command to enable MPLS traffic engineering on an interface, thereby eliminating the need to use the **ip rsvp bandwidth** command. However, if your configuration includes Call Admission Control (CAC) for IPv4 Resource Reservation Protocol (RSVP) flows, you must use the **ip rsvp bandwidth rsvp bandwidth** command.

Examples

The following example shows how to enable MPLS traffic engineering on Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# mpls traffic-eng tunnels
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
mpls traffic-eng tunnels (global configuration)	Enables MPLS traffic engineering tunnel signaling on a device.

mpls ttl-dec

To specify standard Multiprotocol Label Switching (MPLS) tagging, use the **mpls ttl-dec** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mpls ttl-dec
no mpls ttl-dec

Syntax Description

This command has no arguments or keywords.

Command Default

Optimized MPLS tagging (**no mpls ttl-dec**).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

In Cisco IOS Release 12.2(18)SXE and later releases, MPLS tagging has been optimized to allow the rewriting of the original packet's IP type of service (ToS) and Time to Live (TTL) values before the MPLS label is pushed onto the packet header. This change can result in a slightly lower performance for certain types of traffic. If the packet's original ToS/TTL values are not significant, you enter the **mpls ttl-dec** command for standard MPLS tagging.

Examples

This example shows how to configure the Cisco 7600 series router to use standard MPLS tagging behavior:

```
Router(config)# mpls ttl-dec
Router(config)#
```

This example shows how to configure the Cisco 7600 series router to use optimized MPLS tagging behavior:

```
Router(config)# no mpls ttl-dec
Router(config)#
```

Related Commands

Command	Description
mpls l2transport route	Enables routing of Layer 2 packets over MPLS.

mtu

To adjust the maximum packet size or maximum transmission unit (MTU) size, use the **mtu** command in interface configuration mode, connect configuration mode, or xconnect subinterface configuration mode. To restore the MTU value to its original default value, use the **no** form of this command.

mtu *bytes*
no mtu

Syntax Description

bytes	MTU size, in bytes.

Command Default

The table below lists default MTU values according to media type.

Table 1: Default Media MTU Values

Media Type	Default MTU (Bytes)
Ethernet	1500
Serial	1500
Token Ring	4464
ATM	4470
FDDI	4470
HSSI (HSA)	4470

Command Modes

Interface configuration (config-if)
Connect configuration (xconnect-conn-config)
xconnect subinterface configuration (config-if-xconn)

Command History

Release	Modification
10.0	This command was introduced.
12.0(26)S	This command was modified. This command was updated to support the connect configuration mode for Frame Relay Layer 2 interworking.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX. Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Release	Modification
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4. This command supports xconnect subinterface configuration mode.
Cisco IOS XE Release 3.7S	This command was modified as part of the MPLS-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command was made available in template configuration mode.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

Each interface has a default maximum packet size or MTU size. This number generally defaults to the largest size possible for that interface type. On serial interfaces, the MTU size varies but cannot be set to a value less than 64 bytes.

Note The connect configuration mode is used only for Frame Relay Layer 2 interworking.

Changing the MTU Size

Changing the MTU size is not supported on a loopback interface.

Changing the MTU size on a Cisco 7500 series router results in the recarving of buffers and resetting of all interfaces. The following message is displayed: RSP-3-Restart:cbus complex .

You can configure native Gigabit Ethernet ports on the Cisco 7200 series router to a maximum MTU size of 9216 bytes. The MTU values range from 1500 to 9216 bytes. The MTU values can be configured to any range that is supported by the corresponding main interface.

MTU Size for an IPSec Configuration

In an IPSec configuration, such as in a crypto environment, an MTU value that is less than 256 bytes is not accepted. If you configure an MTU value less than 256 bytes, then the MTU value is automatically overwritten and given a value of 256 bytes.

Protocol-Specific Versions of the mtu Command

Changing the MTU value with the **mtu** interface configuration command can affect values for the protocol-specific versions of the command (the **ip mtu** command, for example). If the value specified with the **ip mtu** interface configuration command is the same as the value specified with the **mtu** interface configuration command, and you change the value for the **mtu** interface configuration command, the **ip mtu** value automatically matches the new **mtu** interface configuration command value. However, changing the values for the **ip mtu** configuration commands has no effect on the value for the **mtu** interface configuration command.

ATM and LANE Interfaces

ATM interfaces are not bound by what is configured on the major interface. By default, the MTU on a subinterface is equal to the default MTU (4490 bytes). A client is configured with the range supported by the corresponding main interface. The MTU can be changed on subinterfaces, but it may result in recarving of buffers to accommodate the new maximum MTU on the interface.

VRF-Aware Service Infrastructure Interfaces

The mtu command does not support the VRF-Aware Service Infrastructure (VASI) type interface.

Cisco 7600 Valid MTU Values

On the Cisco 7600 platform, the following valid values are applicable:

- For the SVI ports: from 64 to 9216 bytes
- For the GE-WAN+ ports: from 1500 to 9170 bytes
- For all other ports: from 1500 to 9216 bytes

You can receive jumbo frames on access subinterfaces also. The MTU values can be configured to any range that is supported by the corresponding main interface. If you enable the jumbo frames, the default is 64 bytes for the SVI ports and 9216 bytes for all other ports. The jumbo frames are disabled by default.

Cisco uBR10012 Universal Broadband Router

While configuring the interface MTU size on a Gigabit Ethernet SPA on a Cisco uBR10012 router, consider the following guidelines:

- The default interface MTU size accommodates a 1500-byte packet, plus 22 additional bytes to cover the following overhead:
  - Layer 2 header--14 bytes
  - Dot1Q header--4 bytes
  - CRC--4 bytes
- If you are using MPLS, be sure that the **mpls mtu** command is configured with a value less than or equal to the interface MTU.
- If you are using MPLS labels, you should increase the default interface MTU size to accommodate the number of MPLS labels. Each MPLS label adds 4 bytes of overhead to a packet.

Note For the Gigabit Ethernet SPAs on the Cisco uBR10012 router, the default MTU size is 1500 bytes. When the interface is being used as a Layer 2 port, the maximum configurable MTU is 9000 bytes.

Examples

The following example shows how to specify an MTU of 1000 bytes:

```
Device(config)# interface serial 1
Device(config-if)# mtu 1000
```

Cisco uBR10012 Universal Broadband Router

The following example shows how to specify an MTU size on a Gigabit Ethernet SPA on the Cisco uBR10012 router:

```
Device(config)# interface GigabitEthernet3/0/0
Device(config-if)# mtu 1800
```

The following example shows how to specify an MTU size on a pseudowire interface:

```
Device(config)#  interface pseudowire 100
```

```
Device(config-if)# encapsulation mpls
Device(config-if)# mtu 1800
```

The following example shows how to configure a template and specify an MTU size in template configuration mode: :

```
Device(config)#  template type pseudowire template1
Device(config-if)# encapsulation mpls
Device(config-if)# mtu 1800
```

Related Commands

Command	Description
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
encapsulation smds	Enables SMDS service on the desired interface.
ip mtu	Sets the MTU size of IP packets sent on an interface.

name (MST)

To set the name of a Multiple Spanning Tree (MST) region, use the **name** command in MST configuration submode. To return to the default name, use the **no** form of this command.

name *name*
no name *name*

Syntax Description

name	Name to give the MST region. It can be any string with a maximum length of 32 characters.

Command Default

Empty string

Command Modes

MST configuration (config-mst)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release XE 3.7S	This command was integrated into Cisco IOS XE Release XE 3.7S.

Usage Guidelines

Two or more Cisco 7600 series routers with the same VLAN mapping and configuration version number are considered to be in different MST regions if the region names are different.

Caution Be careful when using the **name** command to set the name of an MST region. If you make a mistake, you can put the Cisco 7600 series router in a different region. The configuration name is a case-sensitive parameter.

Examples

This example shows how to name a region:

```
Device(config-mst)# name Cisco
Device(config-mst)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
revision	Sets the revision number for the MST configuration.
show	Verifies the MST configuration.
show spanning-tree mst	Displays the information about the MST protocol.
spanning-tree mst configuration	Enters MST configuration submode.

neighbor (MPLS)

To specify the peer IP address and virtual circuit (VC) ID value of a Layer 2 VPN (L2VPN) pseudowire, use the **neighbor** command in interface configuration mode. To remove the peer IP address and VC ID value of an L2VPN pseudowire, use the **no** form of this command.

neighbor *peer-address vcid-value*
no neighbor

Syntax Description

peer-address	IP address of the provider edge (PE) peer.
vcid-value	VC ID value. The range is from 1 to 4294967295.

Command Default

Peer address and VC ID value of a pseudowire are not specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the *peer-ip-address* `and` *vc-id* arguments in the **xconnect** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

You must configure the **neighbor** command for the pseudowire to be functional.

Examples

The following example shows how to specify a peer IP address of 10.1.2.3 and VC ID value of 100.

```
Device(config)# interface pseudowire 100
Device(config-if)# neighbor 10.1.2.3 100
```

Related Commands

Command	Description
label (interface pseudowire)	Configures an AToM static pseudowire connection by defining local and remote circuit labels.
neighbor (L2VPN Pseudowire Switching)	Specifies the routers that should form a point-to-point L2 VFI connection.

neighbor activate

To enable the exchange of information with a Border Gateway Protocol (BGP) neighbor, use the **neighbor activate** command in address family configuration mode or router configuration mode. To disable the exchange of an address with a BGP neighbor, use the **no** form of this command.

neighbor {*ip-addresspeer-group-name* | *ipv6-address***%**} **activate**
no neighbor {*ip-addresspeer-group-name* | *ipv6-address***%**} **activate**

Syntax Description

ip-address	IP address of the neighboring router.
peer-group-name	Name of the BGP peer group.
ipv6-address	IPv6 address of the BGP neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.

Command Default

The exchange of addresses with BGP neighbors is enabled for the IPv4 address family. Enabling address exchange for all other address families is disabled.

Note Address exchange for address family IPv4 is enabled by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-activate** command before configuring the **neighbor remote-as** command, or you disable address exchange for address family IPv4 with a specific neighbor by using the **no neighbor activate** command.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
11.0	This command was introduced.
12.0(5)T	Support for address family configuration mode and the IPv4 address family was added.
12.2(2)T	The *ipv6-address* argument and support for the IPv6 address family were added.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **%** keyword was added
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to advertise address information in the form of an IP or IPv6 prefix. The address prefix information is known as Network Layer Reachability Information (NLRI) in BGP.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

Note The use of the **no** form of the **neighbor activate** command will remove all configurations associated with the neighbor both inside and outside address family configuration mode. This command is not the same as the **neighbor shutdown** command, and you should not use this command to disconnect a BGP adjacency.

Address Exchange Example for Address Family vpn4

The following example shows how to enable address exchange for address family vpnv4 for all neighbors in the BGP peer group named PEPEER and for the neighbor 10.0.0.44:

```
Router(config)# address-family vpnv4
Router(config-router-af)# neighbor PEPEER activate
Router(config-router-af)# neighbor 10.0.0.44 activate
Router(config-router-af)# exit-address-family
```

Address Exchange Example for Address Family IPv4 Unicast

The following example shows how to enable address exchange for address family IPv4 unicast for all neighbors in the BGP peer group named group1 and for the BGP neighbor 172.16.1.1:

```
Device(config)# address-family ipv4 unicast
Device(config-router-af)# neighbor group1 activate
Device(config-router-af)# neighbor 172.16.1.1 activate
```

The following example shows how to enable address exchange for address family IPv6 for all neighbors in the BGP peer group named group2 and for the BGP neighbor 7000::2:

```
Device(config)# address-family ipv6
Device(config-router-af)# neighbor group2 activate
Device(config-router-af)# neighbor 7000::2 activate
```

The following example shows that the **no** command will remove all configurations associated with a neighbor both inside and outside the address family configuration mode. The first set of commands shows the configuration for a specific neighbor.

```
Device(config)# router bgp 64496
Device(config-router)# bgp log neighbor changes
Device(config-router)# neighbor 10.0.0.1 remote-as 64497
Device(config-router)# neighbor 10.0.0.1 update-source Loopback0
Device(config-router)# address-family ipv4
Device(config-router-af)# no synchronization
Device(config-router-af)# no neighbor 10.0.0.1 activate
Device(config-router-af)# no auto-summary
Device(config-router-af)# exit-address-family
Device(config-router)address-family vpnv4
Device(config-router-af)# neighbor 10.0.0.1 activate
Device(config-router-af)# neighbor 10.0.0.1 send-community extended
Device(config-router-af)# exit-address-family
Device(config-router)# address-family ipv4 vrf vrf1
Device(config-router-af)# no synchronization
Device(config-router-af)# redistribute connected
Device(config-router-af)# neighbor 192.168.1.4 remote-as 100
Device(config-router-af)# neighbor 192.168.1.4 version 4
Device(config-router-af)# neighbor 192.168.1.4 activate
Device(config-router-af)# neighbor 192.168.1.4 weight 200
Device(config-router-af)# neighbor 192.168.1.4 prefix-list test out
Device(config-router-af)# exit-address-family
```

The following example shows the router configuration after the use of the **no** command.

```
Device(config)# router bgp 64496
Device(config-router)# address-family ipv4 vrf vrf1
Device(config-router-af)# no neighbor 192.168.1.4 activate
01:01:19: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.1.4 IPv4 Unicast vpn vrf vrf1 topology
 base removed from session  Neighbor deleted
01:01:19: %BGP-5-ADJCHANGE: neighbor 192.168.1.4 vpn vrf vrf1 Down Neighbor deleted
Device(config-router-af)# do show running-config | begin router bgp

router bgp 64496
bgp log-neighbor-changes
neighbor 10.0.0.1 remote-as 64496
neighbor 10.0.0.1 update-source Loopback0
!
address-family ipv4
  no synchronization
  no neighbor 10.0.0.1 activate
  no auto-summary
exit-address-family
!
address-family vpnv4
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 send-community extended
exit-address-family
!
address-family ipv4 vrf vrf1
  no synchronization
  redistribute connected
exit-address-family
```

This example shows the router configuration when the neighbor is reactivated.

```
Device(config)# router bgp 64496
```

```
Device(config-router)# address-family ipv4 vrf vrf1
Device(config-router-af)# neighbor 192.168.1.4 activate
01:02:26: %BGP-5-ADJCHANGE: neighbor 192.168.1.4 vpn vrf vrf1 Up
Device(config-router-af)# do show running-config | begin router bgp

router bgp 64496
bgp log-neighbor-changes
neighbor 10.0.0.1 remote-as 64496
neighbor 10.0.0.1 update-source Loopback0
!
address-family ipv4
  no synchronization
  no neighbor 10.0.0.1 activate
  no auto-summary
exit-address-family
!
address-family vpnv4
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 send-community extended
exit-address-family
!
address-family ipv4 vrf vrf1
  no synchronization
  redistribute connected
  neighbor 192.168.1.4 remote-as 100
  neighbor 192.168.1.4 version 4
  neighbor 192.168.1.4 activate
exit-address-family
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.
exit-address-family	Exits from the address family submode.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

neighbor allowas-in

To configure provider edge (PE) routers to allow readvertisement of all prefixes containing duplicate autonomous system numbers (ASNs), use the **neighbor allowas-in** command in router configuration mode. To disable the readvertisement of the ASN of the PE router, use the **no** form of this command.

neighbor *ip-address* **allowas-in** [*number*]
no neighbor allowas-in [*number*]

Syntax Description

ip-address	IP address of the neighboring router.
number	(Optional) Specifies the number of times to allow the advertisement of a PE router's ASN. The range is 1 to 10. If no number is supplied, the default value of 3 times is used.

Command Default

Readvertisement of all prefixes containing duplicate ASNs is disabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.3	This command was integrated into Cisco IOS Release 12.3.
12.3T	This command was integrated into Cisco IOS Release 12.3T.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.4T	This command was integrated into Cisco IOS Release 12.4T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In a hub and spoke configuration, a PE router readvertises all prefixes containing duplicate autonomous system numbers. Use the **neighbor allowas-in** command to configure two VRFs on each PE router to receive and readvertise prefixes are as follows:

- One Virtual Private Network routing and forwarding (VRF) instance receives prefixes with ASNs from all PE routers and then advertises them to neighboring PE routers.
- The other VRF receives prefixes with ASNs from the customer edge (CE) router and readvertises them to all PE routers in the hub and spoke configuration.

You control the number of times an ASN is advertised by specifying a number from 1 to 10.

Examples

The following example shows how to configure the PE router with ASN 100 to allow prefixes from the VRF address family Virtual Private Network (VPN) IPv4 vrf1. The neighboring PE router with the IP address 192.168.255.255 is set to be readvertised to other PE routers with the same ASN six times.

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf vrf1
Router(config-router)# neighbor 192.168.255.255 allowas-in 6
```

Related Commands

Command	Description
address-family	Enters the address family configuration submode used to configure routing protocols such as BGP, OSPF, RIP, and static routing.

neighbor as-override

To configure a provider edge (PE) router to override the autonomous system number (ASN) of a site with the ASN of a provider, use the **neighbor as-override** command in router configuration mode. To remove Virtual Private Network (VPN) IPv4 prefixes from a specified router, use the **no** form of this command.

neighbor *ip-address* **as-override**
no neighbor *ip-address* **as-override**

Syntax Description

ip-address	Specifies the IP address of the router that is to be overridden with the ASN provided.

Command Default

Automatic override of the ASN is disabled.

Command Modes

Router configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used in conjunction with the site-of-origin feature, identifying the site where a route originated, and preventing routing loops between routers within a VPN.

Examples

The following example shows how to configure a router to override the ASN of a site with the ASN of a provider:

```
Router(config)# router bgp 100
Router(config-router)# neighbor 192.168.255.255 remote-as 109
Router(config-router)# neighbor 192.168.255.255 update-source loopback0
Router(config-router)# address-family ipv4 vrf vpn1
Router(config-router)# neighbor 192.168.255.255 activate
Router(config-router)# neighbor 192.168.255.255 as-override
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a BGP neighboring router.
neighbor remote-as	Allows a neighboring router's IP address to be included in the BGP routing table.
neighbor update-source	Allows internal BGP sessions to use any operational interface for TCP/IP connections.
route-map	Redistributes routes from one routing protocol to another.

neighbor inter-as-hybrid

To configure the Exterior Border Gateway Protocol (eBGP) peer router, which is the neighboring Autonomous System Boundary Router (ASBR), as an Inter-AS Option AB peer, use the **neighbor inter-as-hybrid** command in address family configuration mode. The Inter-AS Option AB feature is a hybrid of Inter-AS Option (10)A and Inter-AS Option (10)B network configurations, enabling the interconnection of different autonomous systems to provide Virtual Private Network (VPN) services. To remove the peer router configuration, use the **no** form of this command.

neighbor {*ip-addresspeer-group-name*} **inter-as-hybrid**
no neighbor {*ip-addresspeer-group-name*} **inter-as-hybrid**

Syntax Description

ip-address	The IP address of the Inter-AS AB neighbor.
peer-group-name	The name of a Border Gateway Protocol (BGP) peer group.

Command Default

No Inter-AS AB neighbor eBGP (ASBR) router is specified.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.

Usage Guidelines

Advertised routes have the route targets (RTs) that are configured on the virtual private network (VPN) routing and forwarding (VRF) instance. Advertised routes do not have their original RTs.

If any prefixes are imported into Option AB VRFs, then the imported paths are advertised to this peer.

Examples

The following example shows how to configure an Inter-AS AB neighbor eBGP (ASBR) router:

```
Router(config)# router bgp 100
Router(config-router)# neighbor 192.168.0.1 remote-as 200
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 192.168.0.1 activate
Router(config-router-af)# neighbor 192.168.0.1 inter-as-hybrid
```

Related Commands

Command	Description
address-family vpnv4	Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.

Command	Description
inter-as-hybrid	Specifies a VRF as an Option AB VRF.
neighbor	Adds an entry to the BGP or multiprotocol BGP neighbor table.
neighbor activate	Enables the exchange of information with a neighboring router.

neighbor override-capability-neg

To enable the IPv6 address family for a Border Gateway Protocol (BGP) neighbor that does not support capability negotiation, use the **neighbor override-capability-neg**command in address family configuration mode. To disable the IPv6 address family for a BGP neighbor that does not support capability negotiation, use the **no** form of this command.

neighbor {*peer-group-nameipv6-address*} **override-capability-neg**
no neighbor {*peer-group-nameipv6-address*} **override-capability-neg**

Syntax Description

peer-group-name	Name of a BGP peer group.
ipv6-address	IPv6 address of the BGP neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

Capability negotiation is enabled.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Capability negotiation is used to establish a connection between BGP-speaking peers. If one of the BGP peers does not support capability negotiation, the connection is automatically terminated. The **neighbor override-capability-neg**command overrides the capability negotiation process and enables BGP-speaking peers to establish a connection.

The **neighbor override-capability-neg**command is supported only in address family configuration mode for the IPv6 address family.

Examples

The following example enables the IPv6 address family for BGP neighbor 7000::2:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor 7000::2 override-capability-neg
```

The following example enables the IPv6 address family for all neighbors in the BGP peer group named group1:

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group1 override-capability-neg
```

Related Commands

Command	Description
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.

neighbor remote-as

To add an entry to the BGP or multiprotocol BGP neighbor table, use the **neighbor remote-as** command in router configuration mode. To remove an entry from the table, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address***%***peer-group-name*} **remote-as** *autonomous-system-number* [{**alternate-as** *autonomous-system-number ...*}]
no neighbor {*ip-address* | *ipv6-address***%***peer-group-name*} **remote-as** *autonomous-system-number* [{**alternate-as** *autonomous-system-number ...*}]

Syntax Description

ip-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
peer-group-name	Name of a BGP peer group.
autonomous-system-number	Number of an autonomous system to which the neighbor belongs in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command. When used with the **alternate-as** keyword, up to five autonomous system numbers may be entered.
alternate-as	(Optional) Specifies an alternate autonomous system in which a potential dynamic neighbor can be identified. Up to five autonomous system numbers may be entered when this keyword is specified.

Command Default

There are no BGP or multiprotocol BGP neighbor peers.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.

Release	Modification
11.0	The *peer-group-name* argument was added.
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed.
12.2(4)T	Support for the IPv6 address family was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. The **%** keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH. The **alternate-as** keyword was added to support BGP dynamic neighbors.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Release	Modification
15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the **router bgp** global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only unicast address prefixes. To exchange other address prefix types, such as multicast and Virtual Private Network (VPN) Version 4, neighbors must also be activated in the appropriate address family configuration mode.

Use the **alternate-as** keyword introduced in Cisco IOS Release 12.2(33)SXH to specify up to five alternate autonomous systems in which a dynamic BGP neighbor may be identified. BGP dynamic neighbor support allows BGP peering to a group of remote neighbors that are defined by a range of IP addresses. BGP dynamic neighbors are configured using a range of IP addresses and BGP peer groups. After a subnet range is configured and associated with a BGP peer group using the **bgp listen** command and a TCP session is initiated for an IP address in the subnet range, a new BGP neighbor is dynamically created as a member of that group. The new BGP neighbor will inherit any configuration or templates for the group.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

Note In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

To ensure a smooth transition, we recommend that all BGP speakers within an autonomous system that is identified using a 4-byte autonomous system number, be upgraded to support 4-byte autonomous system numbers.

Examples

The following example specifies that a router at the address 10.108.1.2 is an internal BGP (iBGP) neighbor in autonomous system number 65200:

```
router bgp 65200
 network 10.108.0.0
 neighbor 10.108.1.2 remote-as 65200
```

The following example specifies that a router at the IPv6 address 2001:0DB8:1:1000::72a is an external BGP (eBGP) neighbor in autonomous system number 65001:

```
router bgp 65300
 address-family ipv6 vrf site1
 neighbor 2001:0DB8:1:1000::72a remote-as 65001
```

The following example assigns a BGP router to autonomous system 65400, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 10.108.0.0 and 192.168.7.0 with the neighbor routers. The first router is a remote router in a different autonomous system from the router on which this configuration is entered (an eBGP neighbor); the second **neighbor remote-as** command shows an internal BGP neighbor (with the same autonomous system number) at address 10.108.234.2; and the last **neighbor remote-as** command specifies a neighbor on a different network from the router on which this configuration is entered (also an eBGP neighbor).

```
router bgp 65400
 network 10.108.0.0
 network 192.168.7.0
 neighbor 10.108.200.1 remote-as 65200
 neighbor 10.108.234.2 remote-as 65400
 neighbor 172.29.64.19 remote-as 65300
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only multicast routes:

```
router bgp 65001
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.31 1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
 address-family ipv4 multicast
  neighbor 10.108.1.1 activate
  neighbor 172.31 1.2 activate
  neighbor 172.16.2.2 activate
  exit-address-family
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only unicast routes:

```
router bgp 65001
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.31 1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
```

The following example, configurable only in Cisco IOS Release 12.2(33)SXH and later releases, configures a subnet range of 192.168.0.0/16 and associates this listen range with a BGP peer group. Note that the listen range peer group that is configured for the BGP dynamic neighbor feature can be activated in the IPv4 address family using the **neighbor activate** command. After the initial configuration on Router 1, when Router 2 starts a BGP router session and adds Router 1 to its BGP neighbor table, a TCP session is initiated, and Router 1 creates a new BGP neighbor dynamically because the IP address of the new neighbor is within the listen range subnet.

Router 1

```
enable
configure terminal
router bgp 45000
 bgp log-neighbor-changes
 neighbor group192 peer-group
 bgp listen range 192.168.0.0/16 peer-group group192
 neighbor group192 remote-as 40000 alternate-as 50000
 address-family ipv4 unicast
 neighbor group192 activate
 end
```

Router 2

```
enable
configure terminal
router bgp 50000
 neighbor 192.168.3.1 remote-as 45000
 exit
```

If the **show ip bgp summary** command is now entered on Router 1, the output shows the dynamically created BGP neighbor, 192.168.3.2.

```
Router1# show ip bgp summary
BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1
BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

The following example configures a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain format. This example is supported only on Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or later releases.

```
router bgp 65538
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
```

```
 no auto-summary
 no synchronization
 network 172.17.1.0 mask 255.255.255.0
 exit-address-family
```

The following example configures a BGP process for autonomous system 1.2 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asdot format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3, or a later release.

```
router bgp 1.2
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
bgp listen	Associates a subnet range with a BGP peer group and activates the BGP dynamic neighbors feature.
neighbor peer-group	Creates a BGP peer group.
router bgp	Configures the BGP routing process.

neighbor send-community

To specify that a communities attribute should be sent to a BGP neighbor, use the **neighbor send-community** command in address family or router configuration mode. To remove the entry, use the **no** form of this command.

neighbor {*ip-addressipv6-addresspeer-group-name*} **send-community** [{**both** | **standard** | **extended**}]
no neighbor {*ip-addressipv6-addresspeer-group-name*} **send-community**

Syntax Description

ip-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
peer-group-name	Name of a BGP peer group.
both	(Optional) Specifies that both standard and extended communities will be sent.
standard	(Optional) Specifies that only standard communities will be sent.
extended	(Optional) Specifies that only extended communities will be sent.

Command Default

No communities attribute is sent to any neighbor.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
10.3	This command was introduced.
11.0	The *peer-group-name* argument was added.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The *ipv6-address* argument was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

In the following router configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
 neighbor 172.16.70.23 send-community
```

In the following address family configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
address-family ipv4 multicast
 neighbor 172.16.70.23 send-community
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.
match community	Matches a BGP community.
neighbor remote-as	Creates a BGP peer group.
set community	Sets the BGP communities attribute.

neighbor send-label

To enable a Border Gateway Protocol (BGP) router to send Multiprotocol Label Switching (MPLS) labels with BGP routes to a neighboring BGP router, use the **neighbor send-label** command in address family configuration mode or router configuration mode. To disable this feature, use the **no** form of this command.

neighbor {*ip-addressipv6-addresspeer-group-name*} **send-label** [**explicit-null**]
no neighbor {*ip-addressipv6-addresspeer-group-name*} **send-label** [**explicit-null**]

Syntax Description

ip-address	IP address of the neighboring router.
ipv6-address	IPv6 address of the neighboring router.
peer-group-name	Name of a BGP peer group.
send-label	Sends Network Layer Reachability Information (NLRI) and MPLS labels to this peer.
explicit-null	(Optional) Advertises the Explicit Null label.

Command Default

BGP routers distribute only BGP routes.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was modified. The *ipv6-address* argument was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **neighbor send-label** command enables a router to use BGP to distribute MPLS labels along with IPv4 routes to a peer router. You must issue this command on both the local and the neighboring router.

This command has the following restrictions:

- If a BGP session is running when you issue the **neighbor send-label** command, the BGP session flaps immediately after the command is issued.
- In router configuration mode, only IPv4 addresses are distributed.

Use the **neighbor send-label** command in address family configuration mode, to bind and advertise IPv6 prefix MPLS labels. Using this command in conjunction with the **mpls ipv6 source-interface** global configuration command allows IPv6 traffic to run over an IPv4 MPLS network without any software or hardware configuration changes in the backbone. Edge routers configured to run both IPv4 and IPv6 traffic forward IPv6 traffic using MPLS and multiprotocol internal BGP (MP-iBGP).

Cisco IOS software installs /32 routes for directly connected external BGP (eBGP) peers when the BGP session for such a peer comes up. The /32 routes are installed only when MPLS labels are exchanged between such peers. Directly connected eBGP peers exchange MPLS labels for:

- IP address families (IPv4 and IPv6) with the **neighbor send-label** command enabled for the peers
- VPN address families (VPNv4 and VPNv6)

A single BGP session can include multiple address families. If one of the families exchanges MPLS labels, the /32 neighbor route is installed for the connected peer.

Examples

The following example shows how to enable a router in autonomous system 65000 to send MPLS labels with BGP routes to the neighboring BGP router at 192.168.0.1:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.0.1 remote-as 65001
Router(config-router)# neighbor 192.168.0.1 send-label
```

The following example shows how to enable a router in the autonomous system 65000 to bind and advertise IPv6 prefix MPLS labels and send the labels with BGP routes to the neighboring BGP router at 192.168.99.70:

```
Router(config)# router bgp 65000
Router(config-router)# neighbor 192.168.99.70 remote-as 65000
Router(config-router)# address-family ipv6
Router(config-router-af)# neighbor 192.168.99.70 activate
Router(config-router-af)# neighbor 192.168.99.70 send-label
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
neighbor activate	Enables the exchange of information with a neighboring router.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
mpls ipv6 source-interface	Specifies an IPv6 address of an interface to be used as the source address for locally generated IPv6 packets to be sent over an MPLS network.

neighbor send-label explicit-null

To enable a Border Gateway Protocol (BGP) router to send Multiprotocol Label Switching (MPLS) labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router, use the **neighbor send-label explicit-null** command in address family configuration mode or router configuration mode. To disable a BGP router from sending MPLS labels with explicit-null information, use the **no** form of this command.

neighbor *ip-address* **send-label explicit-null**
no neighbor *ip-address* **send-label explicit-null**

Syntax Description

ip-address	IP address of the neighboring router.

Command Default

None

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command enables a CSC-CE router to use BGP to distribute MPLS labels with a value of zero for explicit-null instead of implicit-null along with IPv4 routes to a CSC-PE peer router.

You must issue this command only on the local CSC-CE router.

You can use this command only with IPv4 addresses.

Examples

In the following CSC-CE example, CSC is configured with BGP to distribute labels and to advertise explicit null for all its connected routes:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# router bgp 100
Router(config-router)# neighbor 10.0.0.2 remote-as 300
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.0.0.2 send-label explicit-null
```

In the following CSC-PE example, CSC is configured with BGP to distribute labels:

```
Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# router bgp 300
Router(config-router)# neighbor 10.0.0.1 remote-as 100
Router(config-router)# address-family ipv4 vrf v1
Router(config-router-af)# neighbor 10.0.0.1 send-label
```

Note Explicit null is not applicable on a CSC-PE router.

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a neighboring router.
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.

neighbor suppress-signaling-protocol

To suppress a Virtual Private LAN Service (VPLS) signaling protocol use the **neighbor suppress-signaling-protocol** command in address family configuration or router configuration mode. To remove the entry, use the **no** form of this command.

neighbor {*ipv4-addressipv6-addresspeer-group-name*} **suppress-signaling-protocol ldp**
no neighbor {*ipv4-addressipv6-addresspeer-group-name*} **suppress-signaling-protocol ldp**

Syntax Description

ipv4-address	IP address of the neighbor.
ipv6-address	IPv6 address of the neighbor.
peer-group-name	Name of a BGP peer group.
ldp	Specifies that Label Distribution Protocol (LDP) signaling will be suppressed.

Command Default

LDP signaling is not suppressed.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

If you specify that LDP signaling is suppressed by using the **ldp** keyword, BGP signaling will be enabled.

Examples

```
Device(config-router-af)# neighbor 10.10.10.1 suppress-signaling-protocol ldp
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.
neighbor remote-as	Creates a BGP peer group.

neighbor update-source

To have the Cisco software allow Border Gateway Protocol (BGP) sessions to use any operational interface for TCP connections, use the **neighbor update-source** command in router configuration mode. To restore the interface assignment to the closest interface, which is called the best local address, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*[{**%**}]*peer-group-name*} **update-source** *interface-type interface-number*
neighbor {*ip-address* | *ipv6-address*[{**%**}]*peer-group-name*} **update-source** *interface-type interface-number*

Syntax Description

ip-address	IPv4 address of the BGP-speaking neighbor.
ipv6-address	IPv6 address of the BGP-speaking neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
peer-group-name	Name of a BGP peer group.
interface-type	Interface type.
interface-number	Interface number.

Command Default

Best local address

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.2(4)T	The *ipv6-address* argument was added.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **%** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command can work in conjunction with the loopback interface feature described in the "Interface Configuration Overview" chapter of the Cisco IOS Interface and Hardware Component Configuration Guide.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

The **neighbor update-source** command must be used to enable IPv6 link-local peering for internal or external BGP sessions.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces and for these link-local IPv6 addresses you must specify the interface they are on. The syntax becomes <IPv6 local-link address>%<interface name>, for example, FE80::1%Ethernet1/0. Note that the interface type and number must not contain any spaces, and be used in full-length form because name shortening is not supported in this situation. The % keyword and subsequent interface syntax is not used for non-link-local IPv6 addresses.

Examples

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface rather than the best local address:

```
router bgp 65000
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 110
 neighbor 172.16.2.3 update-source Loopback0
```

The following example sources IPv6 BGP TCP connections for the specified neighbor in autonomous system 65000 with the global IPv6 address of loopback interface 0 and the specified neighbor in autonomous system 65400 with the link-local IPv6 address of Fast Ethernet interface 0/0. Note that the link-local IPv6 address of FE80::2 is on Ethernet interface 1/0.

```
router bgp 65000
 neighbor 3ffe::3 remote-as 65000
 neighbor 3ffe::3 update-source Loopback0
 neighbor fe80::2%Ethernet1/0 remote-as 65400
 neighbor fe80::2%Ethernet1/0 update-source FastEthernet 0/0
 address-family ipv6
  neighbor 3ffe::3 activate
  neighbor fe80::2%Ethernet1/0 activate
  exit-address-family
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a BGP neighboring router.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

neighbor (VPLS transport mode)

To create pseudowires with specific provider edge (PE) routers in an L2VPN Advanced VPLS configuration, use the **neighbor** command in VPLS transport configuration mode. To remove the pseudowires, use the **no** form of this command.

neighbor *remote-router-id* [**pw-class** *pw-class-name*]
no neighbor *remote-router-id*

Syntax Description

remote-router-id	Remote peer router identifier. The remote router ID can be any IP address, as long as it is reachable.
pw-class	(Optional) Specifies the pseudowire class configuration from which the data encapsulation type is taken.
pw-name-name	Name of the pseudowire class.

Command Default

Pseudowires are not created.

Command Modes

VPLS transport configuration (config-if-transport)

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **neighbor** command uses default values for the VFI name, VPN ID, and encapsulation type.

Examples

The following example shows how two pseudowires are created with PE routers 10.2.2.2 and 10.3.3.3:

```
Router(config)# interface virtual-ethernet 1
Router(config-if)# transport vpls mesh
Router(config-if-transport)# neighbor 10.2.2.2 pw-class 1
Router(config-if-transport)# neighbor 10.3.3.3 pw-class 1
```

Related Commands

Command	Description
transport vpls mesh	Creates a full mesh of pseudowires under a virtual private LAN switching (VPLS) domain.

neighbor (VPLS)

To specify the type of tunnel signaling and encapsulation mechanism for each Virtual Private LAN Service (VPLS) peer, use the **neighbor** command in L2 VFI manual configuration mode. To disable a split horizon, use the **no** form of this command.

neighbor *remote-router-id vc-id* {**encapsulation** *encapsulation-type* | **pw-class** *pw-name*} [**no-split-horizon**]
no neighbor *remote-router-id* [*vc-id*]

Syntax Description

remote-router-id	Remote peer router identifier. The remote router ID can be any IP address, as long as it is reachable.
vc-id	32-bit identifier of the virtual circuit between the routers.
encapsulation	Specifies tunnel encapsulation.
encapsulation-type	Specifies the tunnel encapsulation type; valid values are **l2tpv3** and **mpls**.
pw-class	Specifies the pseudowire class configuration from which the data encapsulation type is taken.
pw-name	Name of the pseudowire class.
no-split-horizon	(Optional) Disables the Layer 2 split horizon forwarding in the data path.

Command Default

Split horizon is enabled.

Command Modes

L2 VFI manual configuration (config-vfi)

Command History

Release	Modification
12.2(18)SXF	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. This command was updated so that the remote router ID need not be the LDP router ID of the peer.
Cisco IOS XE Release XE 3.7S	This command was integrated into Cisco IOS XE Release XE 3.7S.

Usage Guidelines

In a full-mesh VPLS network, keep split horizon enabled to avoid looping.

With the introduction of VPLS Autodiscovery, the remote router ID no longer needs to be the LDP router ID. The address that you specify can be any IP address on the peer, as long as it is reachable. When VPLS Autodiscovery discovers peer routers for the VPLS, the peer router addresses might be any routable address.

Examples

This example shows how to specify the tunnel encapsulation type:

```
Device(config-vfi)# l2 vfi vfi-1 manual
Device(config-vfi)# vpn 1
Device(config-vfi)# neighbor 172.16.10.2 4 encapsulation mpls
```

This example shows how to disable the Layer 2 split horizon in the data path:

```
Device(config-vfi)# l2 vfi vfi-1 manual
Device(config-vfi)# vpn 1
Device(config-vfi)# neighbor 172.16.10.2 4 encapsulation mpls no-split-horizon
```

Related Commands

Command	Description
l2 vfi manual	Creates a Layer 2 VFI.

network (IPv6)

To configure the network source of the next hop to be used by the PE VPN, use the network command in router configuration mode. To disable the source, use the **no** form of this command.

network *ipv6-address/prefix-length*
no network *ipv6-address/prefix-length*

Syntax Description

ipv6-address	The IPv6 address to be used.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

Next-hop network sources are not configured.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The *ipv6-address* argument in this command configures the IPv6 network number.

Examples

The following example places the router in address family configuration mode and configures the network source to be used as the next hop:

```
Router(config)# router bgp 100
Router(config-router)# network 2001:DB8:100::1/128
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions that use standard VPNv6 address prefixes.

next-address

To specify the next IP address in the explicit path, use the **next-address** command in IP explicit path configuration mode.

next-address [{**loose** | **strict**}] *ip-address*

Syntax Description

loose	(Optional) Specifies that the previous address (if any) in the explicit path need not be directly connected to the next IP address, and that the router is free to determine the path from the previous address (if any) to the next IP address.
strict	(Optional) Specifies that the previous address (if any) in the explicit path must be directly connected to the next IP address.
ip-address	Next IP address in the explicit path.

Command Default

The next IP address in the explicit path is not specified.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(19)ST1	The **loose**and **strict** keywords were added.
12.0(21)ST	Support for the Cisco 12000 series router was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

To specify an explicit path that includes only the addresses specified, specify each address in sequence by using the **next-address** command without the **loose** keyword.

To configure an interarea traffic engineering (TE) tunnel, configure the tunnel path options as loose explicit paths. Specify that each Autonomous System Boundary Router (ASBR) traversed by the tunnel label switched path (LSP) is a loose hop by entering the **next-address loose** command.

To use explicit paths for TE tunnels within an Interior Gateway Protocol (IGP) area, you can specify a combination of both loose and strict hops.

When specifying an explicit path for an MPLS TE tunnel, you can specify link or node addresses of the next-hop routers in an explicit path. You can also specify a mixture of link and node addresses. However, there are some restrictions:

- In Cisco IOS Releases 12.2(33)SRD and 12.4(24)T, and Cisco XE Release 2.4 and earlier releases, you cannot specify an explicit path that uses a link address as the first hop and then node addresses as the subsequent hops. However, you can use a node address as the first hop andlink addresses as the subsequent hops.
- In Cisco IOS Releases after 12.2(33)SRD, 12.4(24)T , and Cisco XE Release 2.4, you can use a link address as the first hop and then node addresses as the subsequent hops. There are no restrictions when specifying a mixture of link and node addresses.

When specifying an explicit path, if you specify the "forward" address (the address of the interface that forwards the traffic to the next router) as the next-hop address, the explicit path might not be used. Using the forward address allows that entry to be treated as a loose hop for path calculation. Cisco recommends that you use the "receive"address (the address of the interface that receives traffic from the sending router) as the next-hop address.

In the following example, router R3 sends traffic to router R1. The paths marked a,b and x,y between routers R1 and R2 are parallel paths.

```
R1(a)----(b)R2(c)--(d)R3
  (x)----(y)
```

If you configure an explicit path from R3 to R1 using the "forward" addresses (addresses d and b), the tunnel might reroute traffic over the parallel path (x,y) instead of the explicit path. To ensure that the tunnel uses the explicit path, specify the "receive" addresses as part of the **next-address** command, as shown in the following example:

```
ip explicit-path name path1
  next-address ©)
  next-address (a)
```

Examples

The following example shows how to assign the number 60 to the IP explicit path, enable the path, and specify 10.3.27.3 as the next IP address in the list of IP addresses:

```
Router(config)# ip explicit-path identifier 60 enable
Router(cfg-ip-expl-path)# next-address 10.3.27.3
Explicit Path identifier 60:
    1: next-address 10.3.27.3
```

The following example shows a loose IP explicit path with ID 60. An interarea TE tunnel has a destination of 10.3.29.3 and traverses ASBRs 10.3.27.3 and 10.3.28.3.

```
Router(config)# ip explicit-path identifier 60
Router(cfg-ip-expl-path)# next-address loose 10.3.27.3
Router(cfg-ip-expl-path)# next-address loose 10.3.28.3
Router(cfg-ip-expl-path)# next-address loose 10.3.29.3
```

Related Commands

Command	Description
append-after	Inserts the new path entry after the specified index number.

Command	Description
index	Inserts or modifies a path entry at a specified index.
ip explicit-path	Enters the subcommand mode for IP explicit paths and creates or modifies the specified path.
list	Displays all or part of the explicit paths.
show ip explicit-paths	Displays configured IP explicit paths.

passive-interface (IPv6)

To disable sending routing updates on an interface, use the **passive-interface** command in router configuration mode. To reenable the sending of routing updates, use the **no** form of this command.

passive-interface [{**default** | *interface-type interface-number*}]
no passive-interface [{**default** | *interface-type interface-number*}]

Syntax Description

default	(Optional) All interfaces become passive.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.

Command Default

No interfaces are passive. Routing updates are sent to all interfaces on which the routing protocol is enabled.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(6)T	Support for Enhanced Internal Gateway Routing Protocol (EIGRP) IPv6 was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

If you disable the sending of routing updates on an interface, the particular address prefix will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

OSPF for IPv6 routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF for IPv6 domain.

For the Intermediate System-to-Intermediate System (IS-IS) protocol, this command instructs IS-IS to advertise the IP addresses for the specified interface without actually running IS-IS on that interface. The **no** form of this command for IS-IS disables advertising IP addresses for the specified address.

Examples

The following example sets all interfaces as passive, then activates Ethernet interface 0:

```
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface ethernet0/0
```

oam retry

To configure parameters related to Operation, Administration, and Maintenance (OAM) management for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), VC class, or VC bundle, or label-controlled ATM (LC-ATM) VC, use the **oam retry** command in the appropriate command mode. To remove OAM management parameters, use the **no** form of this command.

oam retry *up-count down-count retry-frequency*
no oam retry

Syntax Description

up-count	Number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to change a connection state to up. This argument does not apply to SVCs.
down-count	Number of consecutive end-to-end F5 OAM loopback cell responses that are not received in order to change the state to down or tear down an SVC connection.
retry-frequency	The frequency (in seconds) at which end-to-end F5 OAM loopback cells are transmitted when a change in the up/down state is being verified. For example, if a PVC is up and a loopback cell response is not received after the *retry-frequency* (in seconds) argument is specified using the **oam-pvc** command, loopback cells are sent at the *retry-frequency* to verify whether the PVC is down.

Command Default

ATM PVCs and SVCs

up-count : 3*down-count*: 5*retry-frequency*: 1 second

LC-ATM VCs

up-count : 2*down-count*: 2*retry-frequency*: 2 seconds

Command Modes

Bundle configuration mode (for a VC bundle)
Control-VC configuration (for an LC-ATM VC)
Interface-ATM-VC configuration (for an ATM PVC or SVC)
PVC range configuration (for an ATM PVC range)
PVC-in-range configuration (for an individual PVC within a PVC range)
VC-class configuration (for a VC class)

Command History

Release	Modification
11.3T	This command was introduced.
12.0(3)T	This command was modified to allow configuration parameters related to OAM management for ATM VC bundles.
12.1(5)T	This command was implemented in PVC range and PVC-in-range configuration modes.
12.3(2)T	This command was implemented in control-VC configuration mode.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The following guidelines apply to PVCs, SVCs, and VC classes. They do not apply to LC-ATM VCs.

- For ATM PVCs, SVCs, or VC bundles, if the **oam retry** command is not explicitly configured, the VC inherits the following default configuration (listed in order of precedence):
  - Configuration of the **oam retry** command in a VC class assigned to the PVC or SVC itself.
  - Configuration of the **oam retry** command in a VC class assigned to the PVC's or SVC's ATM subinterface.
  - Configuration of the **oam retry** command in a VC class assigned to the PVC's or SVC's ATM main interface.
  - Global default: *up-count* = 3, *down-count* = 5, *retry-frequency* = 1 second. This set of defaults assumes that OAM management is enabled using the **oam-pvc** or **oam-svc** command. The *up-count* and *retry-frequency* arguments do not apply to SVCs.
- To use this command in bundle configuration mode, enter the bundle command to create the bundle or to specify an existing bundle before you enter this command.
- If you use the **oam retry** command to configure a VC bundle, you configure all VC members of that bundle. VCs in a VC bundle are further subject to the following inheritance rules (listed in order of precedence):
  - VC configuration in bundle-vc mode
  - Bundle configuration in bundle mode (with the effect of assigned VC-class configuration)
  - Subinterface configuration in subinterface mode

Examples

The following example shows how to configure the OAM management parameters with an up count of 3, a down-count of 3, and the retry frequency set at 10 seconds:

```
Router(cfg-mpls-atm-cvc)# oam retry 3 3 10
```

Related Commands

Command	Description
broadcast	Configures broadcast packet duplication and transmission for an ATM VC class, PVC, SVC, or VC bundle.
class-int	Assigns a VC class to an ATM main interface or subinterface.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
encapsulation	Sets the encapsulation method used by the interface.
inarp	Configures the Inverse ARP time period for an ATM PVC, VC class, or VC bundle.
oam-bundle	Enables end-to-end F5 OAM loopback cell generation and OAM management for a virtual circuit class that can be applied to a virtual circuit bundle.

Command	Description
oam-pvc	Enables end-to-end F5 OAM loopback cell generation and OAM management for an ATM PVC or virtual circuit class.
oam-svc	Enables end-to-end F5 OAM loopback cell generation and OAM management for an ATM SVC or virtual circuit class.
protocol (ATM)	Configures a static map for an ATM PVC, SVC, VC class, or VC bundle. Enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by either configuring Inverse ARP directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only).
ubr	Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
ubr+	Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member.

oam-ac emulation-enable

To enable Operation, Administration, and Maintenance (OAM) cell emulation on ATM adaptation layer 5 (AAL5) over Multiprotocol Label Switching (MPLS) or Layer 2 Tunnel Protocol Version 3 (L2TPv3), use the **oam-ac emulation-enable** command in the appropriate configuration mode on both provider edge (PE) routers. To disable OAM cell emulation, use the **no** form of this command on both routers.

oam-ac emulation-enable [*seconds*]
no oam-ac emulation-enable

Syntax Description

seconds	(Optional) The rate (in seconds) at which the alarm indication signal (AIS) cells should be sent. The range is 0 to 60 seconds. If you specify 0, no AIS cells are sent. The default is 1 second, which means that one AIS cell is sent every second.

Command Default

OAM cell emulation is disabled.

Command Modes

L2transport PVC configuration--for an ATM PVC
VC class configuration mode--for a VC class

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.0(30)S	This command was updated to enable OAM cell emulation as part of a virtual circuit (VC) class.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

This command is used with AAL5 over MPLS or L2TPv3 and is not supported with ATM cell relay over MPLS or L2TPv3.

Examples

The following example shows how to enable OAM cell emulation on an ATM permanent virtual circuit (PVC):

```
Router# interface ATM 1/0/0
Router(config-if)# pvc ½00 l2transport
Router(config-if-atm-l2trans-pvc)# oam-ac emulation-enable
```

The following example shows how to set the rate at which an AIS cell is sent every 30 seconds:

```
Router# interface ATM 1/0/0
Router(config-if)# pvc ½00 l2transport
Router(config-if-atm-l2trans-pvc)# oam-ac emulation-enable 30
```

The following example configures OAM cell emulation for ATM AAL5 over MPLS in VC class configuration mode. The VC class is then applied to an interface.

```
Router> enable
Router# configure terminal
Router(config)# vc-class atm oamclass
Router(config-vc-class)# encapsulation aal5
Router(config-vc-class)# oam-ac emulation-enable 30
Router(config-vc-class)# oam-pvc manage
Router(config)# interface atm1/0
Router(config-if)# class-int oamclass
Router(config-if)# pvc ½00 l2transport
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

Related Commands

Command	Description
show atm pvc	Displays all ATM PVCs and traffic information.

oam-pvc

To enable end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for an ATM permanent virtual circuit (PVC), virtual circuit (VC) class, or label-controlled ATM (LC-ATM) VC, use the **oam-pvc** command in the appropriate command mode. To disable generation of OAM loopback cells and OAM management, use the **no** form of this command.

ATM VC
oam-pvc [{*frequency* | **manage** [*frequency*] [{**auto-detect** [**optimum**] | **keep-vc-up** [**seg aisrdi failure**] | **loop-detection**}]}]
no oam-pvc [{*frequency* | **manage** [*frequency*] [{**auto-detect** [**optimum**] | **keep-vc-up** [**seg aisrdi failure**] | **loop-detection**}]}]

VC Class
oam-pvc [{*frequency* | **manage** [*frequency* [{**auto-detect** [**optimum**] | **loop-detection**}]]}]
no oam-pvc [{*frequency* | **manage** [*frequency* [{**auto-detect** [**optimum**] | **loop-detection**}]]}]

Loopback Mode Detection
oam-pvc manage [*frequency*] **loop-detection**
no oam-pvc manage loop-detection

Cisco 10000 Series Router
oam-pvc [{*frequency* | **manage** [*frequency* [{**auto-detect** [**optimum**] | **keep-vc-up** [**seg aisrdi failure**]}]]}]
no oam-pvc [{*frequency* | **manage** [*frequency* [{**auto-detect** [**optimum**] | **keep-vc-up** [**seg aisrdi failure**]}]]}]

Syntax Description

frequency	(Optional) Specifies the time delay between transmittals of OAM loopback cells, in seconds. For ATM VCs or VC classes and loopback mode detection, the range is 0 to 600, and the default is 10. For LC-ATM VCs, the range is 0 to 255, and the default is 5.
manage	(Optional) for ATM VCs or VC classes; required for LC-ATM VCs) Enables OAM management. The default is disabled.
auto-detect	(Optional) Enables automatic detection of peer OAM command cells.
optimum	(Optional) Configures an optimum mode so that when the traffic-monitoring timer expires, the PVC sends an OAM command cell at the locally configured frequency instead of going into retry mode immediately. If there is no response, the PVC goes into retry mode.
keep-vc-up	(Optional) Specifies that the VC will be kept in the UP state when continuity check (CC) cells detect connectivity failure.
seg aisrdi failure	(Optional) Specifies that if segment alarm indication signal/remote defect indication (AIS/RDI) cells are received, the VC will not be brought down because of end CC failure or loopback failure.

loop-detection	(Optional) Enables automatic detection of whether the physically connected ATM switch is in loopback mode. The default is disabled.

Command Default

OAM management and loop detection are disabled.

Command Modes

ATM VC class configuration (config-vc-class)
ATM VC configuration (config-if-atm-vc)
Control-VC configuration (cfg-mpls-atm-cvc)
PVC-in-range configuration (cfg-if-atm-range-pvc)

Command History

Release	Modification
11.3	This command was introduced.
12.1(5)T	This command was implemented in PVC-in-range configuration mode.
12.3(2)T	This command was implemented for LC-ATM VCs.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S, and the **loop-detection** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(31)SB10	The **loop-detection** keyword was added.
Cisco IOS XE Release 2.3	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

If OAM management is enabled, further control of OAM management is configured by using the **oam retry** command.

ATM VC or VC Classes

If the **oam-pvc** command is not explicitly configured on an ATM PVC, the PVC inherits the following default configuration (in order of precedence):

- Configuration from the **oam-pvc** command in a VC class assigned to the PVC itself.
- Configuration from the **oam-pvc** command in a VC class assigned to the ATM subinterface of the PVC.
- Configuration from the **oam-pvc**command in a VC class assigned to the ATM main interface of the PVC.
- Global default: End-to-end F5 OAM loopback cell generation and OAM management are disabled, but if OAM cells are received, they are looped back. The default value for the *frequency* argument is 10 seconds.

Specifying the ATM VC or VC Classes

You can select the VCs or VC classes to which to apply OAM management and loop detection by using the **oam-pvc** command in any of the following command modes:

- ATM VC class configuration--for a VC class
- ATM VC configuration mode--for an ATM PVC or loopback mode detection
- Control-VC configuration mode--for enabling OAM management on an LC-ATM VC
- PVC-in-range configuration--for an individual PVC within a PVC range

Loopback Mode Detection

When a PVC traverses an ATM cloud and OAM is enabled, the router sends a loopback cell to the other end and waits for a response to determine whether the circuit is up. However, if an intervening router within the ATM cloud is in loopback mode, the router considers the circuit to be up, when in fact the other end is not reachable.

When enabled, the Loopback Mode Detection Through OAM feature detects when an intervening router is in loopback mode, in which case it sets the OAM state to NOT_VERIFIED. This prevents traffic from being routed on the PVC for as long as any intervening router is detected as being in loopback mode.

Examples

The following example shows how to enable end-to-end F5 OAM loopback cell transmission and OAM management on an ATM PVC with a transmission frequency of 3 seconds:

```
Router(cfg-mpls-atm-cvc)# oam-pvc manage 3
```

The following example shows how to enable end-to-end F5 OAM loopback cell transmission and OAM management on an LC-ATM interface with a transmission frequency of 2 seconds:

```
Router(config)# interface Switch1.10 mpls
Router(config-subif)# ip unnumbered Loopback0
Router(config-subif)# mpls atm control-vc 0 32
Router(cfg-mpls-atm-cvc)# oam-pvc manage 2
```

The following example shows how to create a PVC and enable loopback detection:

```
Router(config)# interface ATM1/0
Router(config-if)# pvc 4/100
Router(config-if-atm-vc)# oam-pvc manage loop-detection
```

Related Commands

Command	Description
ilmi manage	Enables ILMI management on an ATM PVC.
oam retry	Configures parameters related to OAM management for an ATM PVC, SVC, VC class, or LC-ATM VC.
show atm pvc	Displays all ATM PVCs and traffic information.

psc refresh interval

To configure the refresh interval for Protection State Coordination (PSC) Protocol messages, use the **psc refresh interval** command in MPLS TP global configuration mode. To remove the configuration, use the **no** form of this command.

psc {**fast** | **slow** | **remote**} **refresh interval** {*time-in-msectime-in-sec*} [**message-count** *num*]
no psc {**fast** | **slow** | **remote**} **refresh interval** {*time-in-msectime-in-sec*} [**message-count** *num*]

Syntax Description

fast	Specifies the fast refresh interval for PSC messages. The default is 1000 ms with a jitter of 50 percent. The range is from 1000 ms to 5000 sec.
slow	Specifies the slow refresh interval for PSC messages. The default is 5 sec. The range is from 5 secs to 86400 secs (24 hours).
remote	Specifies the remote-event expiration timer. By default, this timer is disabled. The remote refresh interval range is from 5 to 86400 sec (24 hours). The message count is from 5 to 1000. If you do not specify the message count value, it is set to 5, which is the default.
message-count *num*	(Optional) Indicates the number of messages.

Command Default

No intervals are specified.

Command Modes

MPLS TP global configuration mode (config-mpls-tp)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

The following example configures a fast refresh interval of 1000 ms.

```
Device(config-mpls-tp)# psc fast refresh interval 1000
```

The following example configures a slow refresh interval of 60 sec.

```
Device(config-mpls-tp)# psc slow refresh interval 60
```

The following example configures a remote refresh interval of 2400 sec and a message count of 10.

```
Device(config-mpls-tp)# psc remote refresh interval 2400 message-count 10
```

Related Commands

Command	Description
emulated-lockout	Enables the sending of emulated lockout commands on working/protection transport entities.

Command	Description
manual-switch	Issues a local manual switch condition on a working LSP.
show mpls tp	Displays a summary of MPLS-TP settings or a detailed list of MPLS-TP tunnels.
debug mpls tp	Enables debugging for MPLS-TP.
clear mpls tp	Clears the counters or a remote event for PSC signaling messages based on a tunnel number or name.

ping mpls

To check Multiprotocol Label Switching (MPLS) label switched path (LSP) connectivity, use the **ping mpls** command in privileged EXEC mode.

ping mpls {**ipv4** *destination-address/destination-mask-length* [{**destination** *address-start address-end increment*}] {**ttl** *time-to-live*} | **pseudowire** *ipv4-address vc-id* [{**segment** [{*segment-number*}]}] [{**destination** *address-start address-end increment*}] | **traffic-eng** *tunnel-interface tunnel-number* [{**ttl** *time-to-live*}]}[{**revision** {**1** | **2** | **3** | **4**}}][{**source** *source-address*}][{**repeat** *count*}][{**timeout** *seconds*}][{**size** *packet-size* | *minimum maximum size-increment*}][{**pad** *pattern*}][{**reply dscp** *dscp-value*}][{**reply pad-tlv**}][{**reply mode** {**ipv4** | **router-alert**}}][{**interval** *ms*}][{**exp** *exp-bits*}][{**verbose**}][{**revision** *tlv-revision-number*}][{**force-explicit-null** }][{**output interface** *tx-interface* [{**nexthop** *ip-address*}]}][{**dsmap** [{**hashkey** {**none** | **ipv4 bitmap** *bitmap-size*}}]}][{**flags fec**}]

Syntax Description

ipv4	Specifies the destination type as a Label Distribution Protocol (LDP) IPv4 address.
destination-address	Address prefix of the target to be tested.
/ *destination-mask-length*	Number of bits in the network mask of the target address. The slash is required.
destination	(Optional) Specifies a network 127 address.
address-start	(Optional) Beginning network 127 address.
address-end	(Optional) Ending network 127 address.
increment	(Optional) Number by which to increment the network 127 address.
ttl *time-to-live*	(Optional) Specifies a time-to-live (TTL) value. The default is 225 seconds.
pseudowire	Specifies the destination type as an Any Transport over MPLS (AToM) virtual circuit (VC).
ipv4-address	IPv4 address of the AToM VC to be tested.
vc-id	Specifies the VC identifier of the AToM VC to be tested.
segment *segment-number*	(Optional) Specifies a segment of a multisegment pseudowire.
traffic-eng	Specifies the destination type as an MPLS traffic engineering (TE) tunnel.
tunnel-interface	Tunnel interface to be tested.
tunnel-number	Tunnel interface number.

revision {**1** | **2** | **3** | **4**}	(Optional) Selects the type, length, values (TLVs) version of the implementation. Use the **revision 4** as the default unless attempting to interoperate with devices running Cisco IOS Release 12.0(27)S1 or 12.0(27)S2. If you do not select a **revision** keyword, the software uses the latest version. See the table in the "Revision Keyword Usage" section of the "Usage Guidelines" section for information on when to select the **1**, **2**, **3**, and **4** keywords.
source *source-address*	(Optional) Specifies the source address or name. The default address is loopback0. This address is used as the destination address in the MPLS echo response.
repeat *count*	(Optional) Specifies the number of times to resend the same packet. The range is 1 to 2147483647. The default is 1. If you do not enter the **repeat** keyword, the software resends the same packet five times.
timeout *seconds*	(Optional) Specifies the timeout interval in seconds for an MPLS request packet. The range is 0 to 3600. The default is 2 seconds.
size *packet-size*	(Optional) Specifies the size of the packet with the label stack imposed. Packet size is the number of bytes in each ping. The range is 40 to 18024. The default is 100.
sweep	(Optional) Enables you to send a number of packets of different sizes, ranging from a start size to an end size. This parameter is similar to the Internet Control Message Protocol (ICMP) **ping sweep** parameter.
minimum	(Optional) Minimum or start size for an MPLS echo packet. The lower boundary of the **sweep** range varies depending on the LSP type. The default is 100 bytes.
maximum	(Optional) Maximum or end size for an echo packet. The default is 17,986 bytes.
size-increment	(Optional) Number by which to increment the echo packet size. The default is 100 bytes.
pad *pattern*	(Optional) The pad TLV is used to fill the datagram so that the MPLS echo request (User Datagram Protocol [UDP] packet with a label stack) is the specified size. The default is 0xABCD.
reply dscp *dscp-value*	(Optional) Provides the capability to request a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value. The echo reply is returned with the IP header type of service (ToS) byte set to the value specified in the **reply dscp** command.
reply pad-tlv	(Optional) Tests the ability of the sender of an echo reply to support the copy pad TLV to echo reply.

reply mode {**ipv4** | **router-alert**}	(Optional) Specifies the reply mode for the echo request packet. **ipv4** --Reply with an IPv4 UDP packet (default). **router-alert** --Reply with an IPv4 UDP packet with router alert.
interval *ms*	(Optional) Specifies the time, in milliseconds (ms), between successive MPLS echo requests. This parameter allows you to pace the transmission of packets so that the receiving router does not drop packets. Default is 0.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for an MPLS echo reply. The range is 0 to 7. Default is 0.
verbose	(Optional) Displays the MPLS echo reply sender address of the packet and displays return codes.
revision *tlv-revision-number*	(Optional) Cisco TLV revision number.
force-explicit-null	(Optional) Forces an explicit null label to be added to the MPLS label stack even though the label was unsolicited.
output interface *tx-interface*	(Optional) Specifies the output interface for echo requests.
nexthop *ip-address*	(Optional) Causes packets to go through the specified next-hop address.
dsmap	(Optional) Interrogates a transit router for downstream mapping (DSMAP) information.
hashkey {**none** | **ipv4 bitmap** *bitmap-size*}	(Optional) Allows you to control the hash key and multipath settings. Valid values are: **none** --There is no multipath (type 0). **ipv4bitmap** *bitmap-size*--Size of the IPv4 addresses (type 8) bitmap. If you enter the **none** keyword, multipath LSP traceroute acts like enhanced LSP traceroute; that is, it uses multipath LSP traceroute retry logic and consistency checking.
flags fec	(Optional) Allows Forward Equivalence Class (FEC) checking on the transit router. A downstream map TLV containing the correct received labels must be present in the echo request for target FEC stack checking to be performed. Target FEC stack validation is always done at the egress router. Be sure to use this keyword with the **ttl** keyword.

Command Default

You cannot check MPLS LSP connectivity.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(18)SXE	The **reply dscp** and **reply pad-tlv** keywords were added.

Release	Modification
12.4(6)T	The following keywords were added: **revision**, **force-explicit-null**, **output interface**, **dsmap**, **hashkey**, **none**, **ipv4 bitmap**, and **flags fec**.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. The **nexthop** keyword was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.3	This command was updated with the **segment** keyword.
12.2(33)SRE	This command was modified. Restrictions were added to the **pseudowire**keyword.
Cisco IOS XE Release 3.6	The **interval** keyword value range changed. The new values are either 0 (default) or from 100 to 3,600,000 ms between successive MPLS echo requests.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Note It is recommended that you use the **mpls oam** global configuration command instead of this command.

Use the **ping mpls** command to validate, test, or troubleshoot IPv4 LDP LSPs, IPv4 Resource Reservation Protocol (RSVP) TE tunnels, and AToM VCs.

With the introduction of Cisco IOS-XE Release 3.6, the **interval** keyword value range changed from 0 to 3,600,000 ms to 0 or 100 to 3,600,000 ms between successive MPLS echo requests.

UDP Destination Address Usage

The destination address is a valid 127/8 address. You have the option to specify a single *x.y.z-address* or a range of numbers from 0.0.0 to *x.y.z* , where *x* , *y* , and *z* are numbers from 0 to 255 and correspond to the 127.*x.y.z* destination address.

The MPLS echo request destination address in the UDP packet is not used to forward the MPLS packet to the destination router. The label stack that is used to forward the echo request routes the MPLS packet to the destination router. The 127/8 address guarantees that the packets are routed to the local host (the default loopback address of the router processing the address) if the UDP packet destination address is used for forwarding.

In addition, the destination address is used to adjust load balancing when the destination address of the IP payload is used for load balancing.

Time-to-Live Usage

The time-to-live value indicates the maximum number of hops a packet should take to reach its destination. The value in the TTL field in a packet is decremented by 1 each time the packet travels through a router.

For MPLS LSP ping, the TTL is a value after which the packet is discarded and an MPLS echo reply is sent back to the originating router.

For MPLS multipath LSP traceroute, the TTL is a maximum time-to-live value and is used to discover the number of downstream hops to the destination router. MPLS LSP traceroute incrementally increases the TTL value in its MPLS echo requests (TTL = 1, 2, 3, 4, ...) to accomplish this.

Downstream Map TLVs

The presence of a downstream map in an echo request is interpreted by the responding transit (not egress) router to include downstream map information in the echo reply. Specify the **ttl** and **dsmap** keywords to cause TTL expiry during LSP ping to interrogate a transit router for downstream information.

Pseudowire Usage

The following keywords are not available with the **ping mpls pseudowire** command:

- **dsmap**
- **flags**
- **force-explicit-null**
- **output**
- **revision**
- **ttl**

The **ping mpls pseudowire** command is not supported when flow label (FAT) is enabled. If you enter the **ping mpls pseudowire** command when FAT is enabled the following message is displayed:

```
% Pseudowire Target Not Supported
```

Revision Keyword Usage

The **revision** keyword allows you to issue a **ping mpls ipv4**, **ping mpls pseudowire**, or **trace mpls traffic-eng** command based on the format of the TLV. The table below lists the revision option and usage guidelines for each option.

Table 2: Revision Options and Option Usage Guidelines

Revision Option	Option Usage Guidelines
1[1]	Not supported in Cisco IOS Release 12.4(11)T or later releases. Version 1 (draft-ietf-mpls-ping-03). For a device running Cisco IOS Release 12.0(27)S3 or a later release, you must use the **revision 1** keyword when you send LSP ping or LSP traceroute commands to devices running Cisco IOS Release 12.0(27)S1 or 12.0(27)S2.
2	Version 2 functionality was replaced by Version 3 functionality before an image was released.

Revision Option	Option Usage Guidelines
3	Version 3 (draft-ietf-mpls-ping-03). • For a device implementing Version 3 (Cisco IOS Release 12.0(27)S3 or a later release), you must use the **revision 1** keyword when you send the LSP **ping** or LSP **traceroute** command to a device implementing Version 1 (that is, either Cisco IOS Release 12.0(27)S1 or Release 12.0(27)S2). • A **ping mpls mpls pseudowire** command does not work with devices running Cisco IOS Release 12.0(27)S1 or Release 12.0(27)S2.
4	• Version 8 (draft-ietf-mpls-ping-08)--Applicable before Cisco IOS Release 12.4(11)T. All echo packet's TLVs are formatted as specified in Version 8. • RFC 4379 compliant--Applicable after Cisco IOS Release 12.4(11)T. All echo packet's TLVs are formatted as specified in RFC 4379.

[1] If you do not specify a revision keyword, the software uses the latest version.

With the introduction of Cisco IOS

Examples

The following example shows how to use the **ping mpls** command to test connectivity of an IPv4 LDP LSP:

```
Router# ping mpls ipv4 10.131.191.252/32 repeat 5 exp 5 verbose
Sending 5, 100-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!     10.131.191.230, return code 3
!     10.131.191.230, return code 3
!     10.131.191.230, return code 3
!     10.131.191.230, return code 3
!     10.131.191.230, return code 3
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/102/112 ms
```

The following example shows how to invoke the **ping mpls** command in the interactive mode to check MPLS LSP connectivity:

```
Router# ping
Protocol [ip]: mpls
Target IPv4, pseudowire or traffic-eng [ipv4]: ipv4
Target IPv4 address: 10.131.159.252
Target mask: 255.255.255.255
Repeat count [5]: 1
Datagram size [100]:
Timeout in seconds [2]:
Send interval in msec [0]:
Extended commands? [no]: yes
Destination address or destination start address: 127.0.0.1
```

```
Destination end address: 127.0.0.1
Destination address increment: 0.0.0.1
Source address:
EXP bits in mpls header [0]:
Pad TLV pattern [ABCD]:
Time To Live [255]:
Reply mode ( 2-ipv4 via udp, 3-ipv4 via udp with router alert) [2]:
Reply ip header DSCP bits [0]:
Verbose mode? [no]: yes
Sweep range of sizes? [no]:
Sending 1, 100-byte MPLS Echos to 10.131.159.252/32,
      timeout is 2 seconds, send interval is 0 msec:
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
Destination address 127.0.0.1
!   10.131.159.245, return code 3
Destination address 127.0.0.1
!   10.131.159.245, return code 3
Destination address 127.0.0.1
!   10.131.159.245, return code 3
Success rate is 100 percent (3/3), round-trip min/avg/max = 40/48/52 ms
```

Note The “Destination end address” and “Destination address increment” prompts display only if you enter an address at the “Destination address or destination start address” prompt. Also, the “Sweep min size,” “Sweep max size,” and “Sweep interval” prompts display only if you enter “yes”at the “Sweep range of sizes? [no]” prompt.

The following example shows how to determine the destination address of an AToM VC:

```
Router# show mpls l2transport vc
Local intf     Local circuit           Dest address    VC ID      Status
-------------  ----------------------- --------------- ---------- ----------
Et2/0          Ethernet                10.131.191.252
 333        UP
Router# show mpls l2transport vc detail
Local interface: Et2/0 up, line protocol up, Ethernet up
  Destination address: 10.131.191.252, VC ID: 333, VC status: up
    Preferred path: not configured
    Default path: active
    Tunnel label: imp-null, next hop 10.131.159.246
    Output interface: Et1/0, imposed label stack {16}
  Create time: 06:46:08, last status change time: 06:45:51
  Signaling protocol: LDP, peer 10.131.191.252:0 up
    MPLS VC labels: local 16, remote 16
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 0, send 0
    byte totals:   receive 0, send 0
    packet drops:  receive 0, send 0
```

This **ping mpls pseudowire** command can be used to test the connectivity of the AToM VC 333 discovered in the preceding **show** command:

```
Router# ping mpls pseudowire 10.131.191.252 333 repeat 200 size 1400
Sending 1, 100-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 92/92/92 ms
```

This ping is particularly useful because the VC might be up and the LDP session between the PE and its downstream neighbor might also be up, but LDP might be configured somewhere in between. In such cases, you can use an LSP ping to verify that the LSP is actually up.

A related point concerns the situation when a pseudowire has been configured to use a specific TE tunnel. For example:

```
Router# show running-config interface ethernet 2/0
Building configuration...
Current configuration : 129 bytes
!
interface Ethernet2/0
 no ip address
 no ip directed-broadcast
 no cdp enable
xconnect 10.131.191.252 333 pw-class test1
end
Router# show running-config
| begin pseudowire
pseudowire-class test1
 encapsulation mpls
 preferred-path interface Tunnel0
```

In such cases, you can use an LSP ping to verify the connectivity of the LSP that a certain pseudowire is taking, be it LDP based or a TE tunnel:

```
Router#

ping mpls pseudowire 10.131.191.252 333 repeat 200 size 1400
Sending 200, 1400-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (200/200), round-trip min/avg/max = 72/85/112 ms
```

You can also use the **ping mpls** command to verify the maximum packet size that can be successfully sent. The following command uses a packet size of 1500 bytes:

```
Router# ping mpls pseudowire 10.131.191.252 333 repeat 5 size 1500
Sending 5, 1500-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
QQQQQ
Success rate is 0 percent (0/5)
```

The Qs indicate that the packets are not sent.

The following command uses a packet size of 1476 bytes:

```
Router# ping mpls pseudowire 10.131.191.252 333 repeat 5 size 1476
Sending 5, 1476-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/83/92 ms
```

The following example shows how to test the connectivity of an MPLS TE tunnel:

```
Router# ping mpls traffic-eng tunnel tun3 repeat 5 verbose
Sending 5, 100-byte MPLS Echos to Tunnel3,
     timeout is 2 seconds, send interval is 0 msec:
Codes:
    '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!   10.131.159.198, return code 3
!   10.131.159.198, return code 3
!   10.131.159.198, return code 3
!   10.131.159.198, return code 3
!   10.131.159.198, return code 3
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/37/40 ms
```

The MPLS LSP ping feature is useful if you want to verify TE tunnels before actually mapping traffic onto them.

The following example shows a **ping mpls** command that specifies segment 2 of a multisegment pseudowire:

```
Router# ping mpls pseudowire 10.131.191.252 333 segment 2
```

Related Commands

Command	Description
mpls oam	Customizes the default behavior of echo packets.
trace mpls	Discovers MPLS LSP routes that packets will actually take when traveling to their destinations.

ping mpls mldp

To check connectivity, isolate failure point, thus providing the Multiprotocol Label Switching (MPLS) Operation, Administration, and Maintenance (OAM) solution, use the **ping mpls mldp** command in privileged EXEC mode.

ping mpls mldp {**mp2mp** | **p2mp**} *root-address* {**ipv4** *source-address group-address* | **ipv6** *source-address group-address* | **mdt** *vpn-id mdt-number* | **vpnv4** *vpn-distinguisher source-address group-address* | **vpnv6** *vpn-distinguisher source-address group-address* | **hex** *opaque-type hex-string*} [{**ddmap** [{**hashkey** {**none** | **ipv4 bitmap** *bitmap-size*}}]}] [{**destination** *address-start address-end* [{*increment increment-mask*}]}] [{**exp** *exp-bits*}] **flags** {**fec** | [{**flags ttl**}] | **ttl** | [{**flags fec**}]} [{**force-explicit-null** }] [{**interval** *delay*}] [{**jitter** *jitter-value*}] [{**output interface** *tx-interface* [{**nexthop** *ip-address*}]}] [{**pad** *pattern*}] [{**repeat** *count*}] [{**reply** {**dscp** *dscp-value* | **mode** | {**ipv4** | **router-alert**}}}] [{**responder-id** *id-address*}] [{**revision** *tlv-revision-number*}] [{**size** *packet-size*}] [{**source** *source-address*}] [{**sweep** *sweep-min-value sweep-max-value sweep-interval*}] [{**timeout** *seconds*}] [{**ttl** *time-to-live*}] [{**verbose**}]

Syntax Description

mp2mp	Checks the connectivity of a multipoint-to-multipoint Multicast Label Distribution Protocol (MLDP) tree from any LSR to egress LSRs (leaves).
p2mp	Checks the connectivity of a point-to-multipoint MLDP tree from ingress LSR (root) to egress LSRs (leaves).
root-address	Specifies MLDP tree root address.
ipv4	Defines IPv4 opaque encoding.
source-address	Specifies the IPv4 source address.
group-address	Specifies the IPv4 group address.
ipv6	Defines IPv6 opaque encoding.
source-address	Specifies the IPv6 source address.
group-address	Specifies the IPv6 group address.
mdt	Defines VPN ID opaque encoding
vpn-id	Specifies the VPN-id. The range of 3-byte OUI is from 0 to 16777215.
mdt-number	Specifies the MDT number. The range is from 0 to 4294967295.
vpnv4	Defines the VPNv4 opaque encoding.
vpn-distinguisher	Specifies the autonomous system number or IP address of VPNv4 route distinguisher.

source-address	Specifies the IPv4 source address.
group-address	Specifies the IPv4 group address.
vpnv6	Defines VPNv6 opaque encoding.
vpn-distinguisher	Specifies the autonomous system number or IP address of VPNv6 route distinguisher.
source-address	Specifies the IPv6 source address.
group-address	Specifies the IPv6 group address.
hex	Allows MLDP forwarding equivalence class (FEC) to be constructed using the type value and the hexadecimal string.
opaque-type	Specifies the type value in the opaque value element of MLDP FEC.
hex-string	Specifies the value in the opaque value element of MLDP FEC.
ddmap	(Optional) Indicates that a downstream detailed mapping TLV (ddmap) must be included in the LSP echo request.
hashkey {**none** | **ipv4 bitmap** *bitmap-size*}	(Optional) Allows you to control the hash key and multipath settings. Valid values are: **none** --There is no multipath (type 0). **ipv4 bitmap** *bitmap-size*--Size of the IPv4 addresses (type 8) bitmap.
destination	(Optional) Specifies a network 127 address.
address-start	(Optional) Specifies the beginning network 127 address.
address-end	(Optional) Specifies an ending network 127 address.
increment	(Optional) Specifies the number by which to increment the destination local host address.
increment-mask	(Optional) Specifies the mask by which to increment the destination local host address.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for an MPLS echo reply. The range is 0 to 7. Default is 0.

flags	(Optional) Allows FEC checking on the transit device. A downstream map TLV containing the correct received labels must be present in the echo request for target FEC stack checking to be performed. Target FEC stack validation is always done at the egress device. Be sure to use this keyword with the **ttl** keyword.
fec	(Optional) Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit devices.
ttl	(Optional) Sets TTL expired flag in the echo request to indicate responder node to respond if echo request was received through TTL expiry.
force-explicit-null	(Optional) Forces an explicit null label to be added to the MPLS label stack even though the label was unsolicited.
interval *delay*	(Optional) Specifies the time, in milliseconds (ms), between successive MPLS echo requests. This parameter allows you to pace the transmission of packets so that the receiving device does not drop packets. Default is 0.
jitter *jitter-value*	(Optional) Configures the jitter value, in milliseconds, that is used in the jitter type, length, values (TLVs) and sent as part of the echo request packets. The range is from 1 to 2147483647. The default is 200.
output interface *tx-interface*	(Optional) Specifies the output interface for echo requests.
nexthop *ip-address*	(Optional) Causes packets to go through the specified next-hop address.
pad *pattern*	(Optional) The pad TLV is used to fill the datagram so that the MPLS echo request (User Datagram Protocol [UDP] packet with a label stack) is the specified size. The default is 0xABCD.
repeat *count*	(Optional) Specifies the number of times to resend the same packet. The range is 1 to 2147483647. The default is 1. If you do not enter the **repeat** keyword, the software resends the same packet five times.

reply dscp *dscp-value*	(Optional) Provides the capability to request a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value. The echo reply is returned with the IP header type of service (ToS) byte set to the value specified in the **reply dscp** command.
reply mode {**ipv4** | **router-alert**}	(Optional) Specifies the reply mode for the echo request packet. **ipv4** --Reply with an IPv4 UDP packet (default). **router-alert** --Reply with an IPv4 UDP packet with router alert.
responder-id *ip-address*	(Optional) Adds responder identifier into corresponding echo request
revision *tlv-revision-number*	(Optional) Cisco TLV revision number.
size *packet-size*	(Optional) Specifies the size of the packet with the label stack imposed. Packet size is the number of bytes in each ping. The range is 72 to 18024. The default is 100.
source *source-address*	(Optional) Specifies the source address or name. The default address is loopback0. This address is used as the destination address in the MPLS echo response.
sweep	(Optional) Specifies sweep range of packet size.
sweep-min-val	(Optional) Specifies the minimum or start size for an MPLS echo packet. The range is from 72 to 18024. The default is 100.
sweep-max-val	(Optional) Specifies the maximum or end size for an MPLS echo packet. The range is from 100 to 18024.
sweep-interval	(Optional) Specifies the sweep interval. The range is from 1 to 8993.
timeout *seconds*	(Optional) Specifies the timeout interval in seconds for an MPLS request packet. The range is 0 to 3600. The default is 2.
ttl *time-to-live*	(Optional) Specifies a time-to-live (TTL) value to be used in the MPLS labels. The default is 225 seconds.
verbose	(Optional) Displays the MPLS echo reply sender address of the packet and displays return codes.

Command Default

You cannot check MPLS LSP connectivity.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Note It is recommended that you use the **mpls oam** global configuration command instead of this command.

Use the **ping mpls mldp** command to check connectivity and isolate failure point, thus providing the Multiprotocol Label Switching (MPLS) Operation, Administration, and Maintenance (OAM) solution.

Destination IP Address Usage

The destination IP address is a localhost 127/8 address. You can specify a single 127/8 IP address or a range of IP addresses between 127.0.0.0 and 127.255.255.255.

Initiator LSR-imposed label stack is used to forward an echo request packet to target(s). Localhost destination IP address used in an MPLS echo request packet is to ensure the packet is never IP routed even if all labels are mistakenly popped along the LSP.

In addition, the destination IP address is used to adjust load balancing when the destination IP address of the IP payload is used for load balancing.

Time-to-Live Usage

The time-to-live value indicates the maximum number of hops a packet should take to reach its destination. The value in the TTL field in a packet is decremented by 1 each time the packet travels through a device.

For MPLS MLDP ping, the TTL is a value after which the packet is discarded and an MPLS echo reply is sent back to the originating device.

Examples

The following example shows how to check connectivity for point-to-multipoint by using the **ping mpls mldp p2mp** command:

```
Device# ping mpls mldp p2mp 10.0.0.5 vpnv4 100:100 38.0.0.8 232.1.1.2
verbose size 200 interval 100 exp 4 timeout 2 repeat 3 jitter 140 ddmap ttl 1

p2mp Root node addr 10.0.0.5
Opaque type VPNv4, source 38.0.0.8, group 232.1.1.2
Sending 3, 200-byte MPLS Echos to Target FEC Stack TLV descriptor,
    timeout is 2.1 seconds, send interval is 100 msec, jitter value is 140 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
```

```
Request #1
L    size 200, reply addr 30.0.0.2, return code 8
Echo Reply received from 30.0.0.2
  DDMAP 0, DS Router Addr 33.0.0.3, DS Intf Addr 33.0.0.3
    RC L, RSC 0, MRU 1500 [Labels: 26 Exp: 4]

  DDMAP 1, DS Router Addr 34.0.0.6, DS Intf Addr 34.0.0.6
    RC L, RSC 0, MRU 1500 [Labels: 26 Exp: 4]

 Received 0 replies

Request #2
L    size 200, reply addr 30.0.0.2, return code 8
Echo Reply received from 30.0.0.2
  DDMAP 0, DS Router Addr 33.0.0.3, DS Intf Addr 33.0.0.3
    RC L, RSC 0, MRU 1500 [Labels: 26 Exp: 4]

  DDMAP 1, DS Router Addr 34.0.0.6, DS Intf Addr 34.0.0.6
    RC L, RSC 0, MRU 1500 [Labels: 26 Exp: 4]

 Received 0 replies

Request #3
L    size 200, reply addr 30.0.0.2, return code 8
Echo Reply received from 30.0.0.2
  DDMAP 0, DS Router Addr 33.0.0.3, DS Intf Addr 33.0.0.3
    RC L, RSC 0, MRU 1500 [Labels: 26 Exp: 4]

  DDMAP 1, DS Router Addr 34.0.0.6, DS Intf Addr 34.0.0.6
    RC L, RSC 0, MRU 1500 [Labels: 26 Exp: 4]

 Received 0 replies

 Total Time Elapsed 6120 ms
```

The following example shows how to check connectivity for multipoint-to-multipoint by using the **ping mpls mldp mp2mp** command:

```
Device#  ping mpls mldp mp2mp 10.0.0.1 mdt 100:100 0
verbose size 200 interval 100 exp 4 timeout 2 repeat 3 jitter 230

mp2mp Root node addr 10.0.0.1
Opaque type MDT, oui:index 0x100:0100, mdtnum 0
Sending 3, 200-byte MPLS Echos to Target FEC Stack TLV descriptor,
    timeout is 2.2 seconds, send interval is 100 msec, jitter value is 230 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'l' - Label switched with FEC change, 'd' - see DDMAP for return code,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

Request #1
!    size 200, reply addr 35.0.0.4, return code 3
!    size 200, reply addr 34.0.0.6, return code 3
!    size 200, reply addr 36.0.0.7, return code 3

Round-trip min/avg/max = 52/92/118 ms
 Received 3 replies
```

```
Request #2
!    size 200, reply addr 34.0.0.6, return code 3
!    size 200, reply addr 36.0.0.7, return code 3
!    size 200, reply addr 35.0.0.4, return code 3

Round-trip min/avg/max = 118/158/196 ms
 Received 3 replies

Request #3
!    size 200, reply addr 36.0.0.7, return code 3
!    size 200, reply addr 34.0.0.6, return code 3
!    size 200, reply addr 35.0.0.4, return code 3

Round-trip min/avg/max = 80/116/155 ms
 Received 3 replies

 Total Time Elapsed 6409 ms
```

Related Commands

Command	Description
mpls oam	Customizes the default behavior of echo packets.
ping mpls	Checks Multiprotocol Label Switching (MPLS) label switched path (LSP) connectivity.

ping mpls tp

To check Multiprotocol Label Switching (MPLS) transport protocol (TP) label switched path (LSP) connectivity, use the **ping mpls tp** command in privileged EXEC mode.

ping mpls tp tunnel-tp *num* **lsp** {**working** | **protect** | **active**} [**ddmap**[{**hashkey ipv4 bitmap** *bitmap-size* | **none**}]] [**dsmap** [{**hashkey ipv4 bitmap** *bitmap-size* | **none**}]] [**destination** *ip-addr*] [**exp** *num*] [**flags fec**] [**interval** *num*] [**pad** *num*] [**repeat** *num*] {[**reply desc** *num*] | [**mode control channel**]} [**size** *num*] [**source** *ip-addr*] [**sweep** *num num num*] [**timeout** *num*] [**ttl** *num*] [**verbose**]

Syntax Description

tunnel-tp *num*	Sepcifies the MPLS-TP tunnel number.
lsp {**working** | **protect** | **active**}	Specifies the type of MPLS-TP label switched path (LSP) on which to send echo request packets.
ddmap [**hashkey ipv4 bitmap** *bitmap-size* | **none**	(Optional) Interrogates a transit router for downstream detailed mapping (DDMAP) information. Allows you to control the hash key and multipath settings.Valid values are: **none** —There is no multipath (type 0). **hashkey ipv4 bitmap** *bitmap-size* —Size of the IPv4 addresses (type 8) bitmap. If you enter the **none** keyword, multipath LSP traceroute acts like enhanced LSP traceroute; that is, it uses multipath LSP traceroute retry logic and consistency checking.
dsmap [**hashkey ipv4 bitmap** *bitmap-size* | **none**	(Optional) Interrogates a transit router for downstream mapping (DSMAP) information. Allows you to control the hash key and multipath settings. Valid values are: **none** —There is no multipath (type 0). **hashkey ipv4 bitmap** *bitmap-size* —Size of the IPv4 addresses (type 8) bitmap. If you enter the **none** keyword, multipath LSP traceroute acts like enhanced LSP traceroute; that is, it uses multipath LSP traceroute retry logic and consistency checking.
destination *ip-addr*	(Optional) Specifies a network 127 address.
exp *num*	(Optional) Specifies the MPLS experimental field value in the MPLS header for an MPLS echo reply. Valid values are from 0 to 7. Default is 0.
flags fec	(Optional) Allows Forward Equivalence Class (FEC) checking on the transit router. A downstream map type, length, variable (TLV) containing the correct received labels must be present in the echo request for target FEC stack checking to be performed. Target FEC stack validation is always done at the egress router. Be sure to use this keyword in conjunction with the **ttl**keyword.

interval *num*	(Optional) Specifies the time, in milliseconds (ms), between successive MPLS echo requests. This parameter allows you to pace the transmission of packets so that the receiving router does not drop packets. Default is 0.
pad *num*	(Optional) The pad TLV is used to fill the datagram so that the MPLS echo request (User Datagram Protocol [UDP] packet with a label stack) is the specified size. The default is 0xABCD.
repeat *num*	(Optional) Specifies the repeat count. Range: 1 to 2147483647.
reply dscp *num* | **mode control channel**	(Optional) Provides the capability to request a specific quality of service (QoS) in an echo reply by providing a differentiated services code point (DSCP) value. The echo reply is returned with the IP header type of service (ToS) byte set to the value specified in the **reply dscp** command.
size *num*	Specifies the packet size.
source *ip-addr*	(Optional) Specifies the source address or name. The default address is loopback0. This address is used as the destination address in the MPLS echo response.
sweep *num num num*	(Optional) Enables you to send a number of packets of different sizes, ranging from a start size to an end size. This parameter is similar to the Internet Control Message Protocol (ICMP) ping sweep parameter.
timeout *num*	(Optional) Specifies the timeout interval in seconds for an MPLS request packet. The range is from 0 to 3600. The default is 2 seconds.
ttl *num*	(Optional) Specifies a time-to-live (TTL) value. The default is 225 seconds.
verbose	(Optional) Enables verbose output mode.

Command Default

Connectivity is not checked.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)SA	This command was introduced.
15.1(3)S	This command was integrated.

Usage Guidelines

Use the **ping mpls tp**command to validate, test, or troubleshoot MPLS TP LSPs.

Note The **ping mpls tp** command does not support interactive mode.

You can use ping and trace in an MPLS-TP network without IP addressing. However, no IP addresses are displayed in the output.

The following rules determine the source IP address:

1. Use the IP address of the TP interface.
2. Use the global router ID.
3. Use the router ID: A.B.C.D local node ID in IPv4 address format. This is not an IP address; however, it is better to use a value rather than leave it as 0.0.0.0 and risk the packet being deemed invalid and dropped.

Examples

The following example checks connectivity of an MPLS-TP LSP:

```
Router# ping mpls tp tunnel-tp 1 repeat 1 ttl 2
Sending 1, 100-byte MPLS Echos to Tunnel-tp1,
     timeout is 2 seconds, send interval is 0 msec:
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 156/156/156 ms
```

Related Commands

Command	Description
trace mpls tp	Displays the MPLS LSP routes that packets take to their destinations.

ping vrf

To test a connection in the context of a specific VPN connection, use the **ping vrf** command in user EXEC or privileged EXEC mode.

ping vrf *vrf-name* [**tag**] [*connection*] *target-address* [*connection-options*]

Syntax Description

vrf-name	The name of the VPN (VRF context).
tag	(Optional) Specifies a tag encapsulated IP (tagIP) ping.
connection	(Optional) Connection options include **atm**, **clns**, **decnet**, **ip**, **ipv6**, **ipx**, **sna**, or **srb**. The default is **ip**.
target-address	The destination ID for the ping operation. Usually, this is the IPv4 address of the host. For example, the target for an IPv4 ping in a VRF context would be the IPv4 address or domain name of the target host. The target for an IPv6 ping in a VRF context would be the IPv6 prefix or domain name of the target host. • If the target address is not specified, the CLI will enter the interactive dialog for ping.
connection-options	(Optional) Each connection type may have its own set of connection options. For example, connection options for IPv4 are **source**, **df-bit**, and **timeout**. See the appropriate **ping** command documentation for details.

Command Default

The default connection type for ping is IPv4.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.1(12c)E, 12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.

Usage Guidelines

A VPN routing and forwarding (VRF) instance is used to identify a VPN. To check if a configured VRF is working, you can use the **ping vrf** command.

When attempting to ping from a provider edge (PE) router to a customer edge (CE) router, or from a PE router to PE router, the standard **ping** command will not usually work. The **ping vrf** command allows you to ping the IP addresses of LAN interfaces on CE routers.

If you are on a PE router, be sure to indicate the specific VRF (VPN) name, as shown in the "Examples" section.

If all required information is not provided at the command line, the system will enter the interactive dialog (extended mode) for ping.

Examples

In the following example, the target host in the domain 209.165.201.1 is pinged (using IP/ICMP) in the context of the "CustomerA" VPN connection.

```
Router# ping vrf CustomerA 209.165.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 176/264/576 ms
```

Pressing the Enter key before providing all of the required options will begin the interactive dialog for ping. In the following example, the interactive dialog is started after the "ip" protocol is specified, but no address is given:

```
Router# ping vrf CustomerB ip

Target IP address: 209.165.200.225
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: Record

Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
Packet has IP options:  Total option bytes= 39, padded length=40
 Record route: <*>
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
   (0.0.0.0)
 .
 .
 .
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

The following example shows the various options for IP in the **ping vrf** command:

```
Router# show parser dump exec | include ping vrf

1 ping vrf <string>
1 ping vrf <string> ip <string>
```

```
1 ping vrf <string> ip (interactive)
1 ping vrf <string> ip <string>
1 ping vrf <string> ip <string> source <address>
1 ping vrf <string> ip <string> source <interface>
1 ping vrf <string> ip <string> repeat <1-2147483647>
1 ping vrf <string> ip <string> size Number
1 ping vrf <string> ip <string> df-bit
1 ping vrf <string> ip <string> validate
1 ping vrf <string> ip <string> data <0-65535>
1 ping vrf <string> ip <string> timeout <0-3600>
1 ping vrf <string> ip <string> verbose
1 ping vrf <string> ip <string> data <0-65535>
1 ping vrf <string> ip <string> timeout <0-3600>
1 ping vrf <string> tag
1 ping vrf <string> atm
1 ping vrf <string> ipv6
1 ping vrf <string> appletalk
1 ping vrf <string> decnet
1 ping vrf <string> clns
1 ping vrf <string> ipx
1 ping vrf <string> sna
1 ping vrf <string> srb
```

Cisco CMTS Routers: Example

The following example shows how to verify the matching and marking configuration in an MPLS network:

```
Router# ping vrf vrfa 1.3.99.98

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.3.99.98, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/20 ms
```

Related Commands

Command	Description
ping	Diagnoses basic network connectivity to a specific host.
ping atm interface atm	Tests the connectivity of a specific PVC.
ping ip	Tests the connection to a remote host on the network using IPv4.
ping ipv6	Tests the connection to a remote host on the network using IPv6.
ping sna	Tests network integrity and timing characteristics over an SNA Switching network.

platform mpls load-balance ingress-port

To improve ingress port-based P router load balancing performance between two Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) line cards, use the **platform mpls load-balance ingress-port** command in global configuration mode. Entering this command will enable this feature. To disable this feature, use the **no** form of the command.

platform mpls load-balance ingress-port
no platform mpls load-balance ingress-port

Syntax Description

This command has no arguments or keywords.

Command Default

Load balancing performance improvements are not enabled .

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was introduced.
15.0M	This command was introduced.

Usage Guidelines

The H-VPLS with Port-Channel Core Interface feature provides support for VPLS to port-channels. You can use this feature to:

- Configure VPLS on the port channel interfaces of the ES+ line card using a load balancing mechanism.
- Match the capabilities and requirements of the VPLS in a single link. Due to multiple links in a link aggregation (LAG), the packets of a particular flow are always transmitted only to one link.
- Configure VPLS with port-channel interfaces as the core facing interface, where the member links of the port-channel are from a ES40 line card. The load-balancing is per-flow based, that is, traffic of a VPLS VC will be load-balanced across member links based on the flow.

Examples

This example shows how to enable improved load-balancing performance on a Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) line card:

```
Router(config)# platform mpls load-balance ingress-port
```

Related Commands

Command	Description
show mpls	Displays information for a line card.

platform mpls mtu-enable

To enable MPLS MTU on the router, use the **platform mpls mtu-enable** command in global configuration mode. To disable this feature, use the **no** form of the command.

platform mpls mtu-enable
no platform mplsmtu-enable

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default .

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.10.2	This command was introduced on the Cisco ASR 900 Series Router.

Usage Guidelines

This command configures MPLS MTU on the router.

Note IP MTU does *not* affect MPLS MTU value.

Note It is *not* recommended to toggle the command as in-consistent MTU values may be displayed.

After configuring or un-configuring the command, it is recommended to re-configure all MTU values on all the interfaces.

Examples

This example shows how to enable MPLS MTU on the Cisco ASR 900 Series Router:

```
Router(config)# platform mpls mtu-enable
Router(config)# interface GigabitEthernet 0/0/1
Router(config-if)# mpls mtu 700
```

Related Commands

Command	Description
show platform hardware pp active feature mpls mtu-table	Displays information MPLS MTU information configured on the router.

policy-map

To enter policy-map configuration mode and create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map**command in global configuration mode. To delete a policy map, use the **no** form of this command.

Supported Platforms Other Than Cisco 10000 and Cisco 7600 Series Routers
policy-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-policy*}] *policy-map-name*
no policy-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-policy*}] *policy-map-name*

Cisco 10000 Series Router
policy-map [**type** {**control** | **service**}] *policy-map-name*
no policy-map [**type** {**control** | **service**}] *policy-map-name*

Cisco CMTS and 7600 Series Router
policy-map [**type** {**class-routing ipv4 unicast** *unicast-name* | **control** *control-name* | **service** *service-name*}] *policy-map-name*
no policy-map [**type** {**class-routing ipv4 unicast** *unicast-name* | **control** *control-name* | **service** *service-name*}] *policy-map-name*

Syntax Description

type	(Optional) Specifies the policy-map type.
stack	(Optional) Determines the exact pattern to look for in the protocol stack of interest.
access-control	(Optional) Enables the policy map for the flexible packet matching feature.
port-filter	(Optional) Enables the policy map for the port-filter feature.
queue-threshold	(Optional) Enables the policy map for the queue-threshold feature.
logging	(Optional) Enables the policy map for the control-plane packet logging feature.
log-policy	(Optional) Type of log policy for control-plane logging.
policy-map-name	Name of the policy map.
control	(Optional) Creates a control policy map.
control-name	Name of the control policy map.
service	(Optional) Creates a service policy map.
service-name	Name of the policy-map service.
class-routing	Configures the class-routing policy map.
ipv4	Configures the class-routing IPv4 policy map.
unicast	Configures the class-routing IPv4 unicast policy map.

unicast-name	Unicast policy-map name.

Command Default

The policy map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.4(4)T	This command was modified. The **type** and**access-control**keywords were added to support flexible packet matching. The **port-filter** and **queue-threshold** keywords were added to support control-plane protection.
12.4(6)T	This command was modified. The **logging** keyword was added to support control-plane packet logging.
12.2(31)SB	This command was modified. The **control** and **service**keywords were added to support the Cisco 10000 series router.
12.2(18)ZY	This command was modified. • The **type** and**access-control**keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series switch that is equipped with the Supervisor 32/programmable intelligent services accelerator (PISA) engine. • The command was modified to enhance the Network-Based Application Recognition (NBAR) functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/PISA engine.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was modified. Support for this command was implemented on Cisco 7600 series routers.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 series routers.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.

Usage Guidelines

Use the **policy-map** command to specify the name of the policy map to be created, added, or modified before you configure policies for classes whose match criteria are defined in a class map. The **policy-map** command enters policy-map configuration mode, in which you can configure or modify the class policies for a policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. Use the **class-map** and **match** commands to configure match criteria for a class. Because you can configure a maximum of 64 class maps, a policy map cannot contain more than 64 class policies, except as noted for quality of service (QoS) class maps on Cisco 7600 systems.

Note For QoS class maps on Cisco 7600 series routers, the limits are 1024 class maps and 256 classes in a policy map.

A policy map containing ATM set cell loss priority (CLP) bit QoS cannot be attached to PPP over X (PPPoX) sessions. The policy map is accepted only if you do not specify the **set atm-clp** command.

A single policy map can be attached to more than one interface concurrently. Except as noted, when you attempt to attach a policy map to an interface, the attempt is denied if the available bandwidth on the interface cannot accommodate the total bandwidth requested by class policies that make up the policy map. In such cases, if the policy map is already attached to other interfaces, the map is removed from those interfaces.

Note This limitation does not apply on Cisco 7600 series routers that have session initiation protocol (SIP)-400 access-facing line cards.

Whenever you modify a class policy in an attached policy map, class-based weighted fair queuing (CBWFQ) is notified and the new classes are installed as part of the policy map in the CBWFQ system.

Note Policy-map installation via subscriber-profile is not supported. If you configure an unsupported policy map and there are a large number of sessions, an equally large number of messages print on the console. For example, if there are 32,000 sessions, then 32,000 messages print on the console at 9,600 baud.

Class Queues (Cisco 10000 Series Routers Only)

The Performance Routing Engine (PRE)2 allows you to configure 31 class queues in a policy map.

In a policy map, the PRE3 allows you to configure one priority level 1 queue, one priority level 2 queue, 12 class queues, and one default queue.

Control Policies (Cisco 10000 Series Routers Only)

Control policies define the actions that your system will take in response to the specified events and conditions.

A control policy is made of one or more control policy rules. A control policy rule is an association of a control class and one or more actions. The control class defines the conditions that must be met before the actions are executed.

There are three steps involved in defining a control policy:

1. Using the **class-map type control** command, create one or more control class maps.
2. Using the **policy-map type control** command, create a control policy map.

A control policy map contains one or more control policy rules. A control policy rule associates a control class map with one or more actions. Actions are numbered and executed sequentially.

1. Using the **service-policy type control** command, apply the control policy map to a context.

Service Policies (Cisco 10000 Series Routers Only)

Service policy maps and service profiles contain a collection of traffic policies and other functions. Traffic policies determine which function is applied to which session traffic. A service policy map or service profile may also contain a network-forwarding policy, which is a specific type of traffic policy that determines how session data packets will be forwarded to the network.

Policy Map Restrictions (Catalyst 6500 Series Switches Only)

Cisco IOS Release 12.2(18)ZY includes software intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine. This release and platform has the following restrictions for using policy maps and **match** commands:

- You cannot modify an existing policy map if the policy map is attached to an interface. To modify the policy map, remove the policy map from the interface by using the **no** form of the **service-policy** command.
- Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application. You can create as many traffic classes as needed. However, the following restrictions apply:
  - A single traffic class can be configured to match a maximum of 8 protocols or applications.
  - Multiple traffic classes can be configured to match a cumulative maximum of 95 protocols or applications.

Examples

The following example shows how to create a policy map called “policy1” and configure two class policies included in that policy map. The class policy called “class1” specifies a policy for traffic that matches access control list (ACL) 136. The second class is the default class to which packets that do not satisfy the configured match criteria are directed.

```
! The following commands create class-map class1 and define its match criteria:
class-map class1
 match access-group 136
! The following commands create the policy map, which is defined to contain policy
! specification for class1 and the default class:
policy-map policy1
class class1
 bandwidth 2000
 queue-limit 40
class class-default
 fair-queue 16
 queue-limit 20
```

The following example shows how to create a policy map called “policy9” and configure three class policies to belong to that map. Of these classes, two specify the policy for classes with class maps that specify match criteria based on either a numbered ACL or an interface name, and one specifies a policy for the default class called “class-default” to which packets that do not satisfy the configured match criteria are directed.

```
policy-map policy9

class acl136
 bandwidth 2000
 queue-limit 40

class ethernet101
 bandwidth 3000
```

```
 random-detect exponential-weighting-constant 10
class class-default
 fair-queue 10
 queue-limit 20
```

The following is an example of a modular QoS command-line interface (MQC) policy map configured to initiate the QoS service at the start of a session.

```
Router> enable
Router# configure terminal
Router(config)# policy-map type control TEST
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 1
 service-policy type service name QoS_Service
Router(config-control-policymap-class-control)# end
```

Examples for Cisco 10000 Series Routers Only

The following example shows the configuration of a control policy map named “rule4”. Control policy map rule4 contains one policy rule, which is the association of the control class named “class3” with the action to authorize subscribers using the network access server (NAS) port ID. The **service-policy type control** command is used to apply the control policy map globally.

```
class-map type control match-all class3
 match vlan 400
 match access-type pppoe
 match domain cisco.com
 available nas-port-id
!
policy-map type control rule4
 class type control class3
  authorize nas-port-id
!
service-policy type control rule4
```

The following example shows the configuration of a service policy map named “redirect-profile”:

```
policy-map type service redirect-profile
 class type traffic CLASS-ALL
  redirect to group redirect-sg
```

Examples for the Cisco CMTS Router

The following example shows how to define a policy map for the 802.1p domain:

```
enable
configure terminal
 policy-map cos7
  class cos7
  set cos 2
  end
```

The following example shows how to define a policy map for the MPLS domain:

```
enable
configure terminal
 policy-map exp7
  class exp7
```

```
set mpls experimental topmost 2
end
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and its default class before you configure its policy.
class class-default	Specifies the default class whose bandwidth is to be configured or modified.
class-map	Creates a class map to be used for matching packets to a specified class.
fair-queue (class-default)	Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
queue-limit	Specifies or modifies the maximum number of packets that the queue can hold for a class policy configured in a policy map.
random-detect (interface)	Enables WRED or DWRED.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detectservice-policy precedence	Configures WRED and DWRED parameters for a particular IP precedence.
service-policy	Attaches a policy map to an input interface or VC or an output interface or VC to be used as the service policy for that interface or VC.
set atm-clp precedence	Sets the ATM CLP bit when a policy map is configured.

preferred-path

To specify the path (a Multiprotocol Label Switching [MPLS] Traffic engineering [TE] tunnel or destination IP address and Domain Name Server [DNS] name) that traffic uses, use the **preferred-path** command in the appropriate configuration mode. To remove path selection, use the **no** form of this command.

preferred-path {[{**interface**}] **tunnel** *tunnel-number* | **peer** *host-ip-address*} [**disable-fallback**]
no preferred-path {**interface tunnel** *tunnel-number* | **peer** *host-ip-address*} [**disable-fallback**]

Syntax Description

interface	Specifies the preferred path using an output interface.
tunnel	Specifies an MPLS TE tunnel interface that is the core-facing output interface.
tunnel-number	The tunnel interface number.
peer	Specifies a destination IP address or DNS name configured on the peer provider edge (PE) router, which is reachable through a label switched path (LSP).
host-ip-address	Peer host name or IP address.
disable-fallback	(Optional) Disables the router from using the default path when the preferred path is unreachable.

Command Default

Path selection is not specified.

Command Modes

Interface configuration (config-if)

Pseudowire class configuration (config-pw-class)

Template configuration (config-template)

Command History

Release	Modification
12.0(25)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.
Cisco IOS XE Release 3.7S	This command was modified as part of the MPLS-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command was made available in interface configuration and template configuration modes.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

The following guidelines provide more information about using this command:

- The destination IP address can be different from the peer router ID used in MPLS Label Distribution Protocol (LDP). For example, a peer PE router can have multiple loopback IP addresses, which can be reached by different paths, such as a TE tunnel, static IP route, or Interior Gateway Protocol (IGP) route.
- This command is available only if the pseudowire encapsulation type is MPLS.
- Tunnel selection is enabled when you exit from pseudowire configuration mode.
- The selected path should be an LSP destined to the peer PE router.
- The selected tunnel must be an MPLS traffic engineering tunnel.
- If you select a tunnel, the tunnel tailend must be on the remote PE router.
- If you specify an IP address, that address must be the IP address of the loopback interface on the remote PE. The address must have a /32 mask.

Examples

The following example shows how to create a pseudowire class and specifies tunnel 1 as the preferred path:

```
Device(config)# pseudowire-class pw1
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# preferred-path interface tunnel 1 disable-fallback
```

The following example shows how to specify tunnel 1 as the preferred path from interface configuration mode:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# preferred-path interface tunnel 1 disable-fallback
```

The following example shows how to specify tunnel 1 as the preferred path from tunnel configuration mode:

```
Device(config)# template type pseudowire template1
Device(config-template)# encapsulation mpls
Device(config-template)# preferred-path interface tunnel 1
```

Related Commands

Command	Description
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
show l2vpn atom vc	Displays information about AToM VCs that have been enabled to route Layer 2 VPN packets on a device.
show mpls l2transport vc	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a device.

priority (LSP Attributes)

To specify the label switched path (LSP) priority in an LSP attribute list, use the **priority** command in LSP Attributes configuration mode. To remove the specified priority, use the **no** form of this command.

priority *setup-priority* [*hold-priority*]
no priority

Syntax Description

setup-priority	Priority used when signaling an LSP to determine which existing LSPs can be preempted. The range is 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.
hold-priority	(Optional) Priority associated with an LSP to determine if it should be preempted by other LSPs that are being signaled. The range is 0 to 7, where a lower number indicates a higher priority.

Command Default

No priority is set in the attribute list.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to configure setup and hold priority for an LSP in an LSP attribute list. Setup priority and hold priority are typically configured to be equal, and setup priority cannot be better (numerically smaller) than the hold priority.

To associate the LSP priority attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example shows how to set the LSP hold and setup property to 0 in an LSP attribute list identified by the string hipriority:

```
configure terminal
!
mpls traffic-eng lsp attributes hipriority
 priority 0 0
 exit
end
```

Related Commands

Command	Description
mpls traffic-end lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

protection (LSP Attributes)

To configure failure protection on the label switched path (LSP) in an LSP attribute list, use the **protection** command in LSP Attributes configuration mode. To disable failure protection, use the **no** form of this command.

protection [**fast reroute** [**bw-protect**]]
no protection

Syntax Description

fast-reroute	Enables an LSP to use an established backup LSP in the event of a link failure.
bw-protect	Enables bandwidth protection.

Command Default

Failure protection is not enabled for the LSP in the LSP attribute list.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to set up LSP failure protection in an LSP attribute list.

To associate the LSP failure protection attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example shows how to enable failure protection on an LSP in an LSP attribute list:

```
configure terminal
!
mpls traffic-eng lsp attributes protect
 protection fast-reroute
 exit
end
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

protection local-prefixes

To enable provider edge (PE)-to-customer edge (CE) link protection by preserving the local label (due to a link failure that caused Border Gateway Protocol (BGP) to begin reconverging), use the **protection local-prefixed** in VRF configuration or in VRF address family configuration mode. To disable this form of link protection, use the **no** form of this command.

protection local-prefixes
no protection local-prefixes

Syntax Description

This command has no arguments or keywords.

Command Default

This protection is disabled by default.

Command Modes

VRF configuration (config-vrf)
VRF address family configuration (config-vrf-af)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS Release 15.0(1)S	This command was modified. Supported was added for PE-CE link protection for IPv6 and this command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

Each Virtual Routing and Forwarding (VRF) that provides protection or a backup path must have a unique route distinguisher (RD) to ensure route reflectors advertise all available paths. Use the **rd** command to specify a route distinguisher for the VRF if none has been created previously.

If your Cisco IOS version includes support for IPv6 and IPv4, use the global configuration **vrf definition** and **rd** commands followed by the **address-family ipv6** or **address-family ipv4** command before you use the **protection local-prefixes**command.

If your Cisco IOS version supports only IPv4, use the global configuration **ip vrf** command before you enter the **rd** and **protection local-prefixes** commands.

If VRF-lite has already been enabled, local protection will not take place. This is true even if entering the **protection local-prefixes** command does not trigger an error message.

Local link protection will only work properly if the failure is quickly detected and an alternate, backup route already exists. Therefore, in addition to the **protection local-prefixes** command, the use of Bidirectional Forwarding Detection (BFD) and topology-specific routing protocols are both required.

Examples

The following example enables local protection in an IPv6-supporting version of Cisco IOS software:

```
vrf definition vrf2
rd 100:3
address-family ipv6
protection local-prefixes
```

The following example enables local protection in an IPv4-only version of Cisco IOS software:

```
ip vrf vpn1
rd 100:3
protection local-prefixes
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enter address family or router scope address family configuration mode to configure a routing session using standard IPv4 address prefixes.
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
bfd interval min_rx multiplier	Sets the BFD session parameters on an interface.
ip vrf	Defines a VPN VRF instance and enters VRF configuration mode.
neighbor fall-over	Enables BGP to monitor the peering session of a specified neighbor for adjacency changes and to deactivate the peering session.
rd	Specifies a RD for a VPN VRF instance.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

pseudowire

To bind a virtual circuit to a Layer 2 pseudowire for an xconnect service, use the **pseudowire** command in interface configuration mode. To remove the binding between a virtual circuit and a Layer 2 pseudowire, use the **no** form of this command.

pseudowire *peer-ip-address vcid* **pw-class** *pw-class-name* [**sequencing** {**transmit** | **receive** | **both**}]
no pseudowire

Syntax Description

peer-ip-address	IP address of the remote peer.
vcid	32-bit identifier of the virtual circuit between devices at each end of a Layer 2 control channel.
pw-class *pw-class-name*	Specifies the pseudowire class configuration from which the data encapsulation type is derived.
sequencing	(Optional) Configures sequencing options for xconnect.
transmit	(Optional) Transmits sequence numbers.
receive	(Optional) Receives sequence numbers.
both	(Optional) Transmits and receives sequence numbers.

Command Default

A virtual circuit is not bound to a Layer 2 pseudowire for an xconnect service.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.2(4)S	This command was modified. The behavior of the **no** form of this command was modified. A configured pseudowire must be disabled before disabling a virtual-ppp interface.

Usage Guidelines

The combination of the *peer-ip-address* and *vcid* arguments must be unique on a device.

The same *vcid* value that identifies a virtual circuit must be configured by using the **pseudowire** command on local and remote devices at each end of a Layer 2 session. The virtual circuit identifier creates a binding between a pseudowire and a virtual circuit.

The **pw-class** *pw-class-name* binds the pseudowire configuration of a virtual circuit to a specific pseudowire class. The pseudowire class configuration serves as a template that contains settings used by all virtual circuits bound to it by using the **pseudowire** command.

When removing a virtual-PPP interface that has a configured pseudowire, you must first remove the pseudowire by using the **no pseudowire** command.

Examples

The following example shows how to create a virtual-PPP interface, configure PPP on the virtual-PPP interface, and bind a virtual circuit to a Layer 2 pseudowire for an xconnect service for a pseudowire class named pwclass1:

```
interface virtual-ppp 1
 ppp authentication chap
 ppp chap hostname peer1
 pseudowire 172.24.13.196 10 pw-class pwclass1
```

The following example shows how to remove a virtual-PPP interface that has a configured pseudowire. You must first remove the configured pseudowire or an error is generated. Note that you can remove the virtual-PPP interface in interface configuration mode as shown below:

```
no interface virtual-ppp 1
% Interface Virtual-PPP1 not removed - Remove the Pseudowire
interface virtual-ppp 1
 no pseudowire
 no interface virtual-ppp 1
 end
```

Related Commands

Command	Description
interface virtual-ppp	Configures a virtual-PPP interface.
l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.
ppp authentication	Enables at least one PPP authentication protocol and specifies the order in which protocols are selected on the interface.
ppp chap hostname	Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP.
pseudowire-class	Specifies the name of a Layer 2 pseudowire class and enters pseudowire class configuration mode.

pseudowire-class

To specify the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode, use the **pseudowire-class** command in global configuration mode. To remove a pseudowire class configuration, use the **no** form of this command.

pseudowire-class *pw-class-name*
no pseudowire-class *pw-class-name*

Syntax Description

pw-class-name	The name of a Layer 2 pseudowire class.

Command Default

No pseudowire classes are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines

The **pseudowire-class** command allows you to configure a pseudowire class template that consists of configuration settings used by all attachment circuits bound to the class. A pseudowire class includes the following configuration settings:

- Data encapsulation type
- Control protocol
- Sequencing
- IP address of the local Layer 2 interface
- Type of service (ToS) value in IP headers

The local interface name for each pseudowire class configured between a pair of PE routers can be the same or different.

After you enter the **pseudowire-class** command, the router switches to pseudowire class configuration mode, where pseudowire settings may be configured.

Examples

The following example shows how to enter pseudowire class configuration mode to configure a pseudowire configuration template named “ether-pw”:

```
Router(config)
# pseudowire-class ether-pw
Router(config-pw)#
```

The following example shows how to enter pseudowire class configuration mode to configure a pseudowire configuration template named “mpls-ip”:

```
Router(config)
# pseudowire-class mpls-ip
```

Related Commands

Command	Description
l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.
pseudowire	Binds an attachment circuit to a Layer 2 pseudowire for xconnect service.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

pseudowire-static-oam class

To create an Operations, Administration, and Maintenance (OAM) class and specify the timeout intervals, use the **pseudowire-static-oam class** command in global configuration mode. To remove the specified class, use the **no** form of this command.

pseudowire-static-oam class *class-name*
no pseudowire-static-oam class *class-name*

Syntax Description

class-name	Name of the class map.

Command Default

OAM classes are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)SA	This command was introduced.
15.1(3)S	This command was integrated.

Usage Guidelines

This command creates an OAM class and enters static pseudowire OAM configuration mode, from which you can enter timeout intervals.

Examples

The following example create the class oam-class3 and enters static pseudowire OAM configuration mode:

```
Router(config)# pseudowire-static-oam class oam-class3
Router(config-st-pw-oam-class)# timeout refresh send  ?
  <1-4095>  Seconds, default is 30
Router(config-st-pw-oam-class)# timeout refresh send  45
```

Related Commands

Command	Description
status protocol notification static	Invokes the specified class as part of the static pseudowire.

pseudowire-tlv template

To create a template of pseudowire type-length-value (TLV) parameters to use in an MPLS-TP configuration, use the **pseudowire-tlv template** command in privileged EXEC configuration mode. To remove the template, use the **no** form of this command.

pseudowire-tlv template *template-name*
no pseudowire-tlv template *template-name*

Syntax Description

template-name	Name for the TLV template.

Command Default

TLV values are not specified.

Command Modes

Privileged EXEC (config#)

Command History

Release	Modification
15.1(1)SA	This command was introduced.
15.1(3)S	This command was integrated.

Examples

The following example shows how to create a TLV template called tlv3:

```
Router(config)# pseudowire-tlv template tlv3
```

Related Commands

Command	Description
tlv template	Specifies a TLV template to use as part of local interface coniguration.

pseudowire routing

To configure Layer 2 VPN (L2VPN) pseudowire routing, use the **pseudowire routing** command in L2VPN configuration mode. To disable L2VPN pseudowire routing configuration, use the **no** form of this command.

pseudowire routing
no pseudowire routing

Syntax Description

This command has no arguments or keywords.

Command Default

L2VPN pseudowire routing is not configured.

Command Modes

L2VPN configuration (config-l2vpn)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **l2 pseudowire routing** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

The **pseudowire routing** command enters Layer 2 pseudowire routing configuration mode (config-l2_pw_rtg), in which you can use additional commands such as the **switching-point** command and the **terminating-pe tie-breaker** command. The **switching-point** command and the **terminating-pe tie-breaker** command are used to configure the L2VPN Virtual Private LAN Services (VPLS) interautonomous systems (Inter-AS) Option B feature. For more information about the L2VPN VPLS Inter-AS Option B feature, see the *Multiprotocol Label Switching Configuration Guide*.

Examples

The following example show how to enable Layer 2 pseudowire routing configuration mode:

```
Device(config)# l2vpn
Device(l2vpn-config)# pseudowire routing
Device(config-l2_pw_rtg)# terminating-pe tie-breaker
Device(config-l2_pw_rtg)# end
```

Related Commands

Command	Description
l2 pseudowire routing	Enter Layer 2 pseudowire routing configuration mode.
switching-point	Configures a switching point and specifies a VC ID range.
terminating-pe tie-breaker	Negotiates the behavior mode (either active or passive) for a TPE router.

pseudowire type

To specify the pseudowire type when configuring pseudowires in a Multiprotocol Label Switching Transport Protocol (MPLS-TP) network, use the **pseudowire type** command in interface configuration mode. To remove the pseudowire type, use the **no** form of this command.

pseudowire type *type-number*
no pseudowire type

Syntax Description

type-number	Type of pseudowire. The range is from 01 to 17 in hexadecimal format.

Command Default

The pseudowire type is not specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the MPLS-based Layer 2 VPN command modifications for cross-OS support. This command will replace the **local interface** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

Pseudowires of type 01 to 17 in hexadecimal format are supported.

Note This command is only available for static pseudowires; that is, this command is only available when the signaling protocol is defined as none.

Examples

The following example shows how to specify a pseudowire of type 16:

```
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# signaling protocol none
Device(config-if)# pseudowire type 16
```

Related Commands

Command	Description
local interface	Specifies the pseudowire type when configuring pseudowires in a MPLS-TP network.

redundancy delay (xconnect)

To specify how long a backup pseudowire should wait before resuming operation after the primary pseudowire goes down, use the **redundancy delay** command in xconnect configuration mode. To remove the specified delay time, use the **no** form of this command.

redundancy delay *enable-delay* {*disable-delay* | **never**}
no redundancy delay *enable-delay* {*disable-delay* | **never**}

Syntax Description

enable-delay	Number of seconds that elapse after the primary pseudowire VC goes down before the Cisco software activates the secondary pseudowire VC. The range is from 0 to 180. The default is 0.
disable-delay	Number of seconds that elapse after the primary pseudowire VC comes up before the Cisco software deactivates the secondary pseudowire VC. The range is from 0 to 180. The default is 0.
never	Specifies that the secondary pseudowire VC will not fall back to the primary pseudowire VC if the primary pseudowire VC becomes available again, unless the secondary pseudowire VC fails.

Command Default

If a failover occurs, the xconnect redundancy algorithm will immediately switch over or fall back to the backup or primary member in the redundancy group.

Command Modes

Xconnect configuration (config-xconnect)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command will replace the **backup delay** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Examples

The following example shows an L2VPN xconnect with one redundant peer. Once a switchover to the secondary pseudowire occurs, there will be no fallback to the primary pseudowire unless the secondary pseudowire fails:

```
Device(config)# l2vpn xconnect context con1
Device(config-xconnect)# redundancy delay 0 never
```

Related Commands

Command	Description
backup delay (L2VPN local switching)	Configures a redundant peer for a pseudowire VC.

redundancy predictive

To enable predictive switchover to a backup pseudowire after the primary pseudowire goes down, use the **redundancy predictive** command in global configuration mode or xconnect configuration mode. To disable redundancy predictive mode, use the **no** form of this command.

redundancy predictive {**enabled** | **disabled**}
no redundancy predictive

Syntax Description

enabled	Enables redundancy predictive mode.
disabled	Disables redundancy predictive mode.

Command Default

Redundancy predictive mode is disabled.

Command Modes

Global configuration mode

Xconnect configuration (config-xconnect)

Command History

Release	Modification
Cisco IOS XE Release 3.10S	This command was introduced.

Examples

The following example shows how to enable redundancy predictive mode in global configuration mode.

```
Device> enable
Device# configure terminal
Device(config)# l2vpn
Device(config-l2vpn)# redundancy predictive enabled
Device(config-l2vpn)# end
```

The following example shows how to enable redundancy predictive mode in xconnect configuration mode.

```
Device> enable
Device# configure terminal
Device(config)# l2vpn xconnect context con1
Device(config-xconnect)# redundancy predictive enabled
Device(config-xconnect)# end
```

rd

To specify a route distinguisher (RD) for a VPN routing and forwarding (VRF) instance, use the **rd**command in VRF configuration mode. To remove a route distinguisher, use the **no** form of this command.

rd *route-distinguisher*
no rd *route-distinguisher*

Syntax Description

route-distinguisher	An 8-byte value to be added to an IPv4 prefix to create a VPN IPv4 prefix.

Command Default

No RD is specified.

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

An RD is either:

- ASN-related--Composed of an autonomous system number and an arbitrary number.

- IP-address-related--Composed of an IP address and an arbitrary number.

You can enter an RD in either of these formats:

- *16-bit autonomous-system-number*:*your 32-bit number*. For example, 101:3.
- *32-bit IP address*:*your 16-bit-number*. For example, 192.168.122.15:1.

Examples

The following example shows how to configure a default RD for two VRFs. It illustrates the use of both autonomous-system-number-relative and IP-address-relative RDs:

```
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:3
Router(config-vrf)# exit
Router(config)# ip vrf vrf2
Router(config-vrf)# rd 10.13.0.12:200
```

The following is an example of a VRF for IPv4 and IPv6 that has common policies defined in the global part of the VRF configuration:

```
vrf definition vrf2
 rd 200:1
 route-target both 200:2
!
 address-family ipv4
 exit-address-family
!
 address-family ipv6
 exit-address-family
 end
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
vrf definition	Configures a VRF routing table and enters VRF configuration mode.

rd (VPLS)

To specify a route distinguisher (RD) to distribute endpoint information in a Virtual Private LAN Service (VPLS) configuration, use the **rd** command in L2 VFI configuration or VFI autodiscovery configuration mode. To remove the manually configured RD and return to the automatically generated RD, use the **no** form of this command.

rd {*autonomous-system-number*:*nn* | *ip-address*:*nn*}
no rd {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

Syntax Description

autonomous-system-number:*nn*	Specifies a 16-bit autonomous system number (ASN) and 32-bit arbitrary number. The ASN does not have to match the local autonomous system number.
ip-address:*nn*	Specifies a 32-bit IP address and a 16-bit arbitrary number. Only IPv4 addresses are supported.

Command Default

VPLS autodiscovery automatically generates a RD using the Border Gateway Protocol (BGP) autonomous system number and the configured virtual forwarding instance (VFI) VPN ID.

Command Modes

L2 VFI configuration (config-vfi)

VFI autodiscovery configuration (config-vfi-autodiscovery)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified as part of the MPLS-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command was made available in VFI autodiscovery configuration mode.

Usage Guidelines

VPLS autodiscovery automatically generates an RD using the BGP autonomous system number and the configured VFI VPN ID. You can use this command to change the automatically generated RD.

The same RD value cannot be configured in multiple VFIs.

There are two formats for configuring the RD argument. It can be configured in the *autonomous-system-number*:*network-number* format, or it can be configured in the *ip-address*:*network-number* format.

An RD is either:

- Autonomous system-related—Composed of an autonomous system number and an arbitrary number.
- IP address-related—Composed of an IP address and an arbitrary number.

You can enter an RD in either of the following formats:

- *16-bit-autonomous-system-number*:*32-bit-number* —For example, 101:3.
- *32-bit-IP-address*:*16-bit-number* —For example, 192.168.122.15:1.

Examples

The following example shows a configuration using VPLS autodiscovery that sets the RD to an IP address of 10.4.4.4 and a network address of 70:

```
Device(config)# l2 vfi SP2 autodiscovery
Device(config-vfi)# vpn id 200
Device(config-vfi)# vpls-id 10.4.4.4:70
Device(config-vfi)# rd 10.4.5.5:7
```

The following example shows a configuration using VPLS Autodiscovery that sets the RD to an autonomous system number of 2 and a network address of 3:

```
Device(config)# l2 vfi SP2 autodiscovery
Device(config-vfi)# vpn id 200
Device(config-vfi)# vpls-id 10.4.4.4:70
Device(config-vfi)# rd 2:3
```

The following example shows a configuration using VPLS autodiscovery that sets the RD to an autonomous system number of 2 and a network address of 3 in VFI autodiscovery configuration mode:

```
Device(config)# l2vpn vfi context vfi1
Device(config-vfi)# vpn id 200
Device(config-vfi)# autodiscovery bgp signaling ldp
Device(config-vfi-autodiscovery)# rd 2:3
```

Related Commands

Command	Description
autodiscovery (l2vpn vfi)	Designates VFI as having BGP autodiscovered pseudowire members.
l2 vfi autodiscovery	Enables a VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain.

record-route (LSP Attributes)

To record the route used by the label switched path (LSP), use the **record-route**command in LSP Attributes configuration mode. To stop the recording the route used by the LSP, use the **no** form of this command.

record-route
no record-route

Syntax Description

This command has no arguments or keywords.

Command Default

The LSP route is not recorded.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to set up in an LSP attribute list the recording of the route taken by the LSP.

To associate the LSP record-route attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example shows how to set up LSP route recording in an LSP attribute list:

```
configure terminal
!
mpls traffic-eng lsp attributes 9
 record-route
 exit
end
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

revision

To set the revision number for the Multiple Spanning Tree (802.1s) (MST) configuration, use the **revision** command in MST configuration submode. To return to the default settings, use the **no** form of this command.

revision *version*
no revision

Syntax Description

version	Revision number for the configuration; valid values are from 0 to 65535.

Command Default

version is **0**

Command Modes

MST configuration (config-mst)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release XE 3.7S	This command was integrated into Cisco IOS XE Release XE 3.7S.

Usage Guidelines

Two Cisco 7600 series routers that have the same configuration but different revision numbers are considered to be part of two different regions.

Caution Be careful when using the **revision** command to set the revision number of the MST configuration because a mistake can put the switch in a different region.

Examples

This example shows how to set the revision number of the MST configuration:

```
Device(config-mst)# revision 5
Device(config-mst)#
```

Related Commands

Command	Description
instance	Maps a VLAN or a set of VLANs to an MST instance.
name (MST configuration submode)	Sets the name of an MST region.
show	Verifies the MST configuration.
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree mst configuration	Enters MST-configuration submode.

router-id

To specify a Layer 2 VPN (L2VPN) router ID for the provider edge (PE) router to use with Virtual Private LAN Services (VPLS) autodiscovery pseudowires, use the **router-id** command in L2VPN configuration mode. To reset the command to the default configuration, use the **no** form of this command.

router-id *ip-address*
no router-id *ip-address*

Syntax Description

ip-address	Router ID in IP address format.

Command Default

The L2VPN router ID is set to the Multiprotocol Label Switching (MPLS) global router ID.

Command Modes

L2VPN configuration (config-l2vpn)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **l2 router-id** command in future releases.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique.

The L2VPN router ID is used in the forward equivalence class (FEC) 129 encoding for pseudowire signaling. It is also used in the network layer reachability information (NLRI) for peer discovery.

Examples

The following example shows how to specify an L2VPN router ID:

```
Device(config)# l2vpn
Device(config-l2vpn)# router-id 10.1.1.1
```

Related Commands

Command	Description
l2 router-id	Specifies a router ID for the PE router to use with VPLS autodiscovery pseudowires.

route-target

To create a route-target extended community for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **route-target** command in VRF configuration or in VRF address family configuration mode. To disable the configuration of a route-target community option, use the **no** form of this command.

route-target [{**import** | **export** | **both**}] *route-target-ext-community*
no route-target [{**import** | **export** | **both**}] [*route-target-ext-community*]

Syntax Description

import	(Optional) Imports routing information from the target VPN extended community.
export	(Optional) Exports routing information to the target VPN extended community.
both	(Optional) Imports both import and export routing information to the target VPN extended community.
route-target-ext-community	The route-target extended community attributes to be added to the VRF's list of import, export, or both (import and export) route-target extended communities.

Command Default

A VRF has no route-target extended community attributes associated with it.

Command Modes

VRF address family configuration (config-vrf-af)
VRF configuration (config-vrf)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was modified. Support for IPv6 was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers was changed to asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers was changed to asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 3.3SG	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.1(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The **route-target** command creates lists of import and export route-target extended communities for the specified VRF. Enter the command one time for each target community. Learned routes that carry a specific route-target extended community are imported into all VRFs configured with that extended community as an import route target. Routes learned from a VRF site (for example, by Border Gateway Protocol (BGP), Routing Information Protocol (RIP), or static route configuration) contain export route targets for extended communities configured for the VRF added as route attributes to control the VRFs into which the route is imported.

The route target specifies a target VPN extended community. Like a route distinguisher, an extended community is composed of either an autonomous system number and an arbitrary number or an IP address and an arbitrary number. You can enter the numbers in either of these formats:

- 16-bit autonomous-system-number:your 32-bit number. For example, 101:3.
- 32-bit IP address:your 16-bit number. For example, 192.168.122.15:1.

Note In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538, for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2, for example--as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following example shows how to configure route-target extended community attributes for a VRF in IPv4. The result of the command sequence is that VRF named vrf1 has two export extended communities (1000:1 and 1000:2) and two import extended communities (1000:1 and 10.27.0.130:200):

```
ip vrf vrf1
 route-target both 1000:1
 route-target export 1000:2
 route-target import 10.27.0.130:200
```

The following example shows how to configure route-target extended community attributes for a VRF that includes IPv4 and IPv6 address families:

```
vrf definition site1
rd 1000:1
address-family ipv4
 route-target export 100:1
 route-target import 100:1
address-family ipv6
 route-target export 200:1
 route-target import 200:1
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases shows how to create a VRF with a route target that uses a 4-byte autonomous system number in asplain format--65537--and how to set the route target to extended community value 65537:100 for routes that are permitted by the route map:

```
ip vrf vrf1
 rd 64500:100
 route-target both 65537:100
 exit
route-map vrf1 permit 10
 set extcommunity rt 65537:100
 end
```

After the configuration is completed, use the **show route-map** command to verify that the extended community is set to the route target containing the 4-byte autonomous system number of 65537:

```
Router# show route-map vrf1
route-map vrf1, permit, sequence 10
  Match clauses:
  Set clauses:
    extended community RT:65537:100
  Policy routing matches: 0 packets, 0 bytes
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, shows how to create a VRF with a route target that uses a 4-byte autonomous system number in asdot format--1.1--and how to set the route target to extended community value 1.1:100 for routes that are permitted by the route map:

```
ip vrf vrf1
 rd 64500:100
 route-target both 1.1:100
 exit
route-map vrf1 permit 10
 set extcommunity rt 1.1:100
 end
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
clear ip bgp	Resets Border Gateway Protocol (BGP) connections using hard or soft reconfiguration.
import map	Configures an import route map for a VRF.
ip vrf	Configures a VRF routing table.
vrf definition	Configures a VRF routing table and enters VRF configuration mode.

route-target (VPLS)

To specify a route target for a Virtual Private LAN Services (VPLS) virtual forwarding instance (VFI), use the **route-target** command in L2 VFI configuration or VFI auto discovery configuration mode. To revert to the automatically generated route target, use the **no** form of this command.

route-target [{**import** | **export** | **both**}] {*autonomous-system-number*:*nn* | *ip-address*:*nn*}
no route-target {**import** | **export** | **both**} {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

Syntax Description

import	(Optional) Imports routing information from the target VPN extended community.
export	(Optional) Exports routing information to the target VPN extended community.
both	(Optional) Imports and exports routing information to the target VPN extended community.
autonomous-system-number:*nn*	Specifies the autonomous system number (ASN) and a 32-bit number.
ip-address:*nn*	Specifies the IP address and a 16-bit number.

Command Default

VPLS Autodiscovery automatically generates a route target using the lower six bytes of the route distinguisher (RD) and VPLS ID.

Command Modes

L2 VFI configuration (config-vfi)

VFI autodiscovery configuration (config-vfi-autodiscovery)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified as part of the MPLS-based Layer 2 VPN (L2VPN) command modifications for cross-OS support . This command was made available in VFI autodiscovery configuration mode.

Usage Guidelines

The same route target cannot be configured in multiple VFIs.

The route target specifies a target VPN extended community. Like a route distinguisher, an extended community is composed of either an autonomous system number and an arbitrary number or an IP address and an arbitrary number. You can enter the numbers in either of the following formats:

- *16-bit-autonomous-system-number*:*32-bit-number*—For example, 101:3.
- *32-bit-IP-address*:*16-bit-number* —For example, 192.168.122.15:1.

Examples

The following example shows how to configure VPLS autodiscovery route-target extended community attributes for VFI SP1:

```
Device(config)# l2 vfi SP1 autodiscovery
Device(config-vfi)# vpn id 100
Device(config-vfi)# vpls-id 5:300
Device(config-vfi)# rd 4:4
Device(config-vfi)# route-target 10.1.1.1:29
```

The following example shows how to configure VPLS autodiscovery route-target extended community attributes for VFI vfi1:

```
Device(config)# l2vpn vfi context vfi1
Device(config-vfi)# vpn id 100
Device(config-vfi)# autodiscovery bgp signaling ldp
Device(config-vfi-autodiscovery)# rd 4:4
Device(config-vfi-autodiscovery)# route-target 10.1.1.1:29
```

Related Commands

Command	Description
autodiscovery (l2vpn vfi)	Designates VFI as having BGP autodiscovered pseudowire members.
auto-route-target	Automatically generates the route target in a VFI.
l2 vfi autodiscovery	Enables a VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain.

router bgp

To configure the Border Gateway Protocol (BGP) routing process, use the **router bgp** command in global configuration mode. To remove a BGP routing process, use the **no** form of this command.

router bgp *autonomous-system-number*
no router bgp *autonomous-system-number*

Syntax Description

autonomous-system-number	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the "Usage Guidelines" section.

Command Default

No BGP routing process is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was modified. Support for IPv6 was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(33)SB	This command was modified. Support for IPv6 was added.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 3.3SG	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

This command allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Prior to January 2009, BGP autonomous system numbers that were allocated to companies were 2-octet numbers in the range from 1 to 65535 as described in RFC 4271, *A Border Gateway Protocol 4 (BGP-4)* . Due to increased demand for autonomous system numbers, the Internet Assigned Number Authority (IANA) will start in January 2009 to allocate four-octet autonomous system numbers in the range from 65536 to 4294967295. RFC 5396, *Textual Representation of Autonomous System (AS) Numbers* , documents three methods of representing autonomous system numbers. Cisco has implemented the following two methods:

- Asplain—Decimal value notation where both 2-byte and 4-byte autonomous system numbers are represented by their decimal value. For example, 65526 is a 2-byte autonomous system number and 234567 is a 4-byte autonomous system number.
- Asdot—Autonomous system dot notation where 2-byte autonomous system numbers are represented by their decimal value and 4-byte autonomous system numbers are represented by a dot notation. For example, 65526 is a 2-byte autonomous system number and 1.169031 is a 4-byte autonomous system number (this is dot notation for the 234567 decimal number).

For details about the third method of representing autonomous system numbers, see RFC 5396.

Note In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

Asdot Only Autonomous System Number Formatting

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, the 4-octet (4-byte) autonomous system numbers are entered and displayed only in asdot notation, for example, 1.10 or 45000.64000. When using regular expressions to match 4-byte autonomous system numbers the asdot format includes a period which is a special character in regular expressions. A backslash must be entered before the period for example, 1\.14, to ensure the regular expression match does not fail. The table below shows the format in which 2-byte and 4-byte autonomous system numbers are configured, matched in regular expressions, and displayed in **show** command output in Cisco IOS images where only asdot formatting is available.

Table 3: Asdot Only 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535

Asplain as Default Autonomous System Number Formatting

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain as the default display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain and asdot format. In addition, the default format for matching 4-byte autonomous system numbers in regular expressions is asplain, so you must ensure that any regular expressions to match 4-byte autonomous system numbers are written in the asplain format. If you want to change the default **show** command output to display 4-byte autonomous system numbers in the asdot format, use the **bgp asnotation dot** command under router configuration mode. When the asdot format is enabled as the default, any regular expressions to match 4-byte autonomous system numbers must be written using the asdot format, or the regular expression match will fail. The tables below show that although you can configure 4-byte autonomous system numbers in either asplain or asdot format, only one format is used to display **show** command output and control 4-byte autonomous system number matching for regular expressions, and the default is asplain format. To display 4-byte autonomous system numbers in **show** command output and to control matching for regular expressions in the asdot format, you must configure the **bgp asnotation dot** command. After enabling the **bgp asnotation dot** command, a hard reset must be initiated for all BGP sessions by entering the **clear ip bgp *** command.

Note If you are upgrading to an image that supports 4-byte autonomous system numbers, you can still use 2-byte autonomous system numbers. The **show** command output and regular expression match are not changed and remain in asplain (decimal value) format for 2-byte autonomous system numbers regardless of the format configured for 4-byte autonomous system numbers.

Table 4: Default Asplain 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 65536 to 4294967295
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 65536 to 4294967295

Table 5: Asdot 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535

Reserved and Private Autonomous System Numbers

In Cisco IOS Release 12.0(32)S12, 12.0(32)SY8, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3 and later releases, the Cisco implementation of BGP supports RFC 4893. RFC 4893 was developed to allow BGP to support a gradual transition from 2-byte autonomous system numbers to 4-byte autonomous system numbers. A new reserved (private) autonomous system number, 23456, was created by RFC 4893 and this number cannot be configured as an autonomous system number in the Cisco IOS CLI.

RFC 5398, *Autonomous System (AS) Number Reservation for Documentation Use* , describes new reserved autonomous system numbers for documentation purposes. Use of the reserved numbers allow configuration examples to be accurately documented and avoids conflict with production networks if these configurations are literally copied. The reserved numbers are documented in the IANA autonomous system number registry. Reserved 2-byte autonomous system numbers are in the contiguous block, 64496 to 64511 and reserved 4-byte autonomous system numbers are from 65536 to 65551 inclusive.

Private 2-byte autonomous system numbers are still valid in the range from 64512 to 65534 with 65535 being reserved for special use. Private autonomous system numbers can be used for internal routing domains but must be translated for traffic that is routed out to the Internet. BGP should not be configured to advertise private autonomous system numbers to external networks. Cisco IOS software does not remove private autonomous system numbers from routing updates by default. We recommend that ISPs filter private autonomous system numbers.

Note Autonomous system number assignment for public and private networks is governed by the IANA. For information about autonomous-system numbers, including reserved number assignment, or to apply to register an autonomous system number, see the following URL: http://www.iana.org/.

Examples

The following example configures a BGP process for autonomous system 45000 and configures two external BGP neighbors in different autonomous systems using 2-byte autonomous system numbers:

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

The following example configures a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain notation. This example is supported i n Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases.

```
router bgp 65538
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

The following example configures a BGP process for autonomous system 1.2 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asdot notation. This example is supported in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, and Cisco IOS XE Release 2.3, and later releases.

```
router bgp 1.2
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

Command	Description
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.